Manual do usuário

AWS License Manager

AWS License Manager: Manual do usuário

Table of Contents

O que AWS License Manageré

AWS License Manager facilita o gerenciamento de licenças de software de fornecedores de software (por exemplo, Microsoft, SAP, Oracle e IBM) em várias AWS regiões e contas dentro de uma organização, oferecendo visibilidade consolidada e relatórios abrangentes para conformidade de licenças de software em grande escala. Isso permite que você limite os excedentes de licenciamento e reduza o risco de não conformidade e relatórios incorretos.

Ao criar sua infraestrutura de nuvem AWS, você pode economizar custos usando as oportunidades do modelo Bring Your Own License (BYOL). Ou seja, você poderá reaproveitar o inventário de licenças existente para usar com atributos de nuvem.

O License Manager reduz o risco de excedentes e penalidades de licenciamento com o rastreamento de inventário vinculado diretamente aos serviços. AWS Com controles baseados em regras no consumo de licenças, os administradores podem definir limites rígidos ou flexíveis em implantações de nuvem novas e existentes. Com base nesses limites, o License Manager ajuda a impedir o uso incompatível do servidor antes que isso aconteça.

Os painéis integrados do License Manager fornecem visibilidade contínua do uso de licenças e assistência nas auditorias de fornecedores.

O License Manager suporta o rastreamento de qualquer software licenciado com base em núcleos virtuais (vCPUs), núcleos físicos, soquetes ou número de máquinas. Isso inclui uma variedade de produtos de software da Microsoft, IBM, SAP, Oracle e outros fornecedores.

Com AWS License Manager, você pode rastrear licenças de forma centralizada e impor limites em várias regiões, mantendo uma contagem de todos os direitos retirados. O License Manager também rastreia a identidade do usuário e o identificador de atributo subjacente, se disponível, associado a cada check-out, além de quando o check-out foi feito. Esses dados de séries temporais podem ser rastreados até o ISV por meio de CloudWatch métricas e eventos. ISVs pode usar esses dados para análises, auditorias e outros fins semelhantes.

AWS License Manager é integrado AWS Marketplaceao AWS Data Exchange e aos seguintes AWS serviços: AWS Identity and Access Management (IAM) AWS Organizations, Service Quotas CloudFormation, marcação de AWS recursos e. AWS X-Ray

Direitos gerenciados

Com o License Manager, um administrador de licenças pode distribuir, ativar e rastrear licenças de software em todas as contas e em toda a organização.

Fornecedores independentes de software (ISVs) podem usar AWS License Manager para gerenciar e distribuir licenças e dados de software para usuários finais por meio de direitos gerenciados. Como emissor, você pode monitorar centralmente o uso de suas licenças emitidas pelo vendedor usando o painel do License Manager. ISVs a venda por meio do AWS Marketplace benefício da criação e distribuição automáticas de licenças como parte do fluxo de trabalho da transação. ISVs também pode usar o License Manager para criar chaves de licença e ativar licenças para clientes sem uma AWS conta.

O License Manager usa padrões abertos e seguros do setor para representar licenças e permite que os clientes verifiquem criptograficamente sua autenticidade. O License Manager oferece suporte a uma variedade de modelos de licenciamento diferentes, incluindo licenças perpétuas, licenças flutuantes, licenças por assinatura e licenças baseadas no uso. Se você tiver licenças que precisam ser bloqueadas por nó, o License Manager fornece mecanismos para consumir as licenças dessa forma.

Você pode criar licenças AWS License Manager e distribuí-las aos usuários finais usando uma identidade do IAM ou por meio de tokens assinados digitalmente gerados por. AWS License Manager Os usuários finais que usam AWS podem redistribuir ainda mais os direitos de licença às AWS identidades em suas respectivas organizações. Usuários finais com direitos distribuídos podem fazer check-out e check-in dos direitos exigidos pela licença por meio de integração de seu software com o AWS License Manager. Cada check-out de licença especifica os direitos, a quantidade associada e o período de check-out, como o check-out de 10 **`admin-users`** por 1 hora. Essa verificação pode ser realizada com base na identidade subjacente do IAM para a licença distribuída ou com base nos tokens de longa duração gerados por AWS License Manager meio do AWS License Manager serviço.

Casos de uso do License Manager

Veja a seguir exemplos da funcionalidade fornecida pelo License Manager para vários casos de uso:

- Licenças autogerenciadas no License Manager— Usado para definir regras de licenciamento para licenças autogerenciadas em uma única AWS conta com base nos termos de seus contratos

corporativos. Para cenários com várias contas, considere usar grupos de ativos de licenças para uma governança centralizada.

- Grupos de ativos de licença— Usado para gerenciar e rastrear centralmente licenças em várias AWS regiões e contas dentro de uma organização.
- Licenças emitidas pelo vendedor no License Manager: usado para gerenciar e distribuir licenças de software para usuários finais.
- Licenças concedidas no License Manager— Usado para controlar o uso de licenças adquiridas de AWS Marketplace AWS Data Exchange, ou diretamente de um vendedor que integrou seu software com direitos gerenciados. Pode ser gerenciado individualmente em contas únicas ou centralmente em várias contas usando grupos de ativos de licença.
- Conversões de tipo de licença no License Manager— Usado para alterar seu tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) sem reimplantar suas cargas de trabalho.
- Pesquisa de inventário no License Manager— Usado para descobrir e rastrear aplicativos locais usando regras de AWS Systems Manager inventário e licenciamento.
- Use assinaturas baseadas no usuário do License Manager para produtos de software compatíveis: usado para comprar licenças totalmente compatíveis fornecidas pela Amazon para software com suporte a uma taxa de assinatura por usuário.
- Gerencie assinaturas Linux no License Manager: usado para visualizar e gerenciar assinaturas comerciais do Linux que você possui e executa na AWS.

Serviços relacionados

O License Manager é integrado com Amazon EC2, Amazon RDS, AWS Marketplace, AWS Systems Manager, e. AWS Organizations

A EC2 integração com a Amazon permite que você acompanhe as licenças dos seguintes recursos e aplique as regras de licenciamento em todo o ciclo de vida do recurso:

- EC2Instâncias da Amazon
- Instâncias dedicadas
- Hosts dedicados
- Instâncias spot e frota spot
- Nós gerenciados

Ao usar o License Manager junto com AWS Systems Manager, você pode gerenciar licenças em servidores físicos ou virtuais hospedados fora do AWS. Você pode usar o License Manager com AWS Organizations para gerenciar todas as suas contas organizacionais de forma centralizada.

Além disso, você pode controlar o uso de licenças compradas de AWS Marketplace AWS Data Exchange, ou diretamente de um vendedor que integrou seu software com. AWS License Manager Você pode usar AWS License Manager para distribuir direitos de uso, conhecidos como direitos, para pessoas específicas. Contas da AWS

O License Manager se integra ao Amazon RDS for Oracle e ao Amazon RDS para licenças BYOL baseadas em vCPUs do Db2. Com essa integração, você ganha visibilidade do uso da vCPU para suas instâncias de banco de dados RDS for Oracle e RDS for Db2. Você pode usar esses dados para calcular o número de licenças consumidas com base nos termos de licenciamento com os fornecedores do sistema de gerenciamento de banco de dados. Para obter mais informações, consulte os seguintes links associados no Guia do usuário do Amazon RDS.

- Opções de licenciamento do RDS para Oracle
- Opções de licenciamento do RDS for Db2

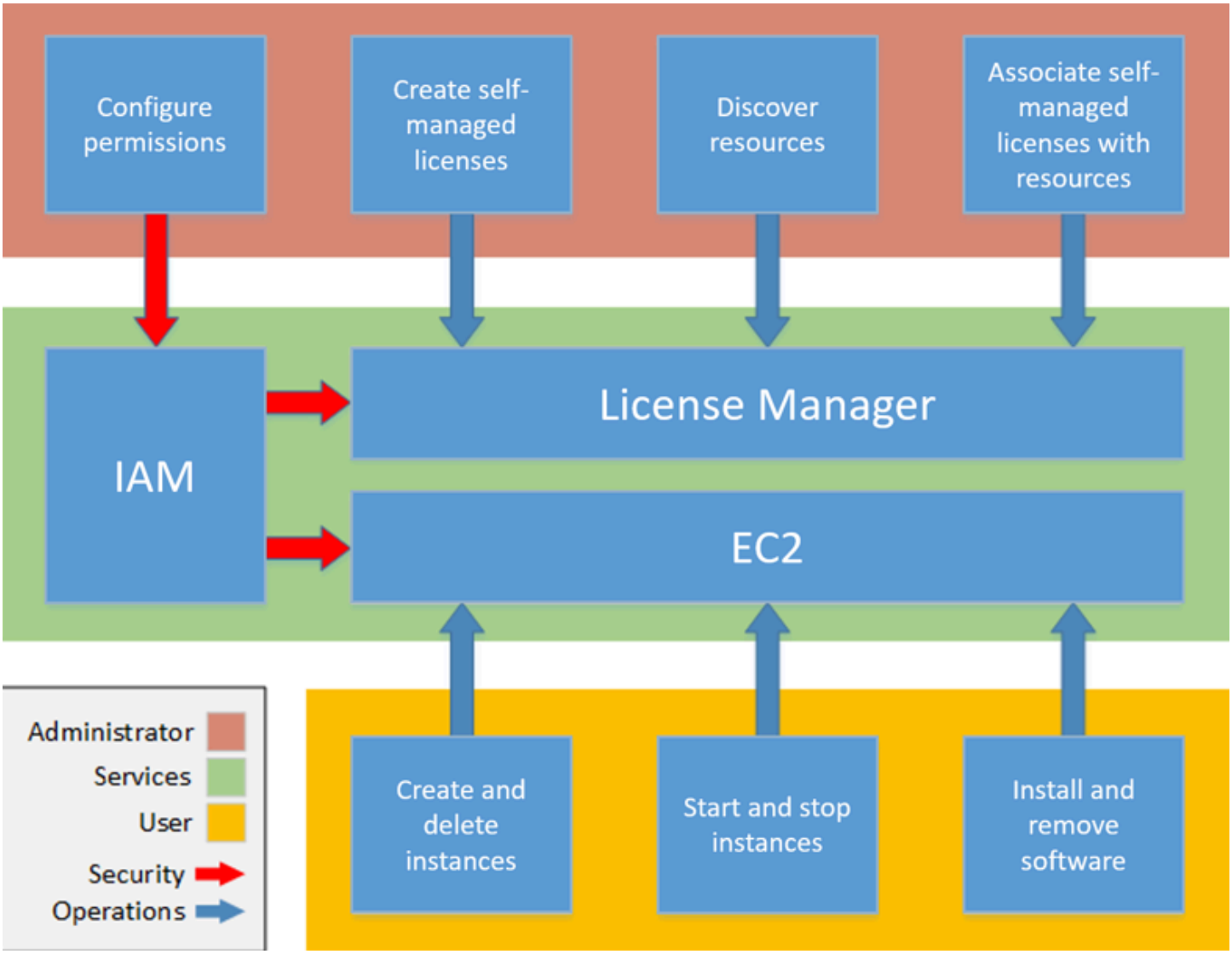
Como o License Manager funciona

O gerenciamento eficaz de licenças de software depende do seguinte:

- Uma compreensão especializada da linguagem em contratos de licenciamento corporativo
- Acesso adequadamente restrito às operações que consomem licenças
- Rastreamento preciso do inventário de licenças

É provável que as empresas tenham pessoas ou equipes dedicadas responsáveis por cada um desses domínios. Depois isso se torna um problema de comunicação eficaz, principalmente entre especialistas em licenças e administradores de sistemas. O License Manager apresenta uma forma de reunir conhecimento de vários domínios. Fundamentalmente, ele também se integra de forma nativa aos AWS serviços, por exemplo, com o plano de EC2 controle da Amazon, onde as instâncias são criadas e excluídas. Isso significa que as regras e limites do License Manager capturam o conhecimento comercial e operacional e também se convertem em controles automatizados na criação de instâncias e na implantação de aplicativos.

O diagrama a seguir ilustra as funções distintas, mas coordenadas, dos administradores de licenças, que gerenciam as permissões e configuram o License Manager, e dos usuários, que criam, gerenciam e excluem recursos por meio do console da Amazon EC2 .



Se for responsável pelo gerenciamento de licenças em sua organização, você poderá usar o License Manager para definir regras de licenciamento, anexá-las a seus lançamentos e rastrear o uso. Os usuários em sua organização podem adicionar e remover atributos que consomem licença sem trabalho adicional.

Os grupos de ativos de licenças ampliam esse recurso fornecendo gerenciamento de licenças em toda a organização que funciona em várias AWS regiões e contas. Em vez de gerenciar licenças individualmente em cada região e conta, os grupos de ativos de licenças consolidam as informações de licenciamento em visualizações unificadas, permitindo a supervisão centralizada e o monitoramento automatizado da conformidade em toda a sua organização. AWS

Um especialista em licenciamento gerencia licenças em toda a organização, determinando as necessidades de inventário de atributos, supervisionando a aquisição de licenças e orientando o

uso de licenças em conformidade. Em uma empresa que usa o License Manager, esse trabalho é consolidado por meio do console do License Manager. Conforme mostrado no diagrama, isso envolve a definição de permissões de serviço, a criação de licenças autogerenciadas, o inventário de atributos de computação on-premises e na nuvem e a associação de licenças autogerenciadas a atributos descobertos. Com os grupos de ativos de licenças, os especialistas em licenciamento também podem criar grupos de licenças centralizados que descobrem e rastreiam automaticamente o software em todas as regiões e contas, reduzindo a sobrecarga administrativa do gerenciamento de licenças em grande escala. Na prática, isso pode significar associar uma licença autogerenciada a uma Amazon Machine Image (AMI) aprovada que a TI usa como modelo para todas as implantações de EC2 instâncias da Amazon.

O License Menager economiza custos que, de outra forma, seriam perdidos em violações de licenças. Auditorias internas revelam violações apenas após o fato, quando é tarde demais para evitar penalidades por incompatibilidade. O Licence Manager impede que esses incidentes caros aconteçam. O License Manager simplifica a criação de relatórios com painéis integrados que mostram o consumo de licenças e os atributos monitorados.

Grupos de ativos de licenças no fluxo de trabalho de gerenciamento de licenças

Os grupos de ativos de licenças fornecem uma camada adicional de organização e automação ao fluxo de trabalho de gerenciamento de licenças. Enquanto as configurações tradicionais de licenças funcionam no nível de licença individual, os grupos de ativos de licenças operam no nível organizacional, fornecendo visualizações consolidadas e gerenciamento automatizado em várias regiões e contas.

Relacionamento com os recursos existentes do License Manager

Os grupos de ativos de licenças complementam e aprimoram os recursos existentes do License Manager:

- Configurações de licença - os grupos de ativos de licenças podem incorporar configurações de licenças autogerenciadas e licenças concedidas, fornecendo uma visão unificada, independentemente de como as licenças foram originalmente criadas ou adquiridas.
- Pesquisa de inventário - os grupos de ativos de licenças usam os mesmos mecanismos de descoberta da pesquisa de inventário, mas automatizam o agrupamento e o monitoramento contínuo dos recursos descobertos com base em conjuntos de regras.

- Relatórios de uso - grupos de ativos de licenças geram relatórios abrangentes que abrangem várias regiões e contas, fornecendo visibilidade em toda a organização que relatórios de licenças individuais não conseguem alcançar.
- Gerenciamento entre contas - Os grupos de ativos de licenças são projetados especificamente para cenários de várias contas, trabalhando perfeitamente com AWS Organizations para fornecer governança centralizada de licenças.

Cenários de casos de uso de grupos de ativos de licença

Os grupos de ativos de licenças são particularmente valiosos nos seguintes cenários:

- Implantações em várias regiões — quando sua organização executa cargas de trabalho em várias AWS regiões e precisa de um controle consolidado de licenças sem gerenciar cada região separadamente.
- Organizações com várias contas - Ao usar AWS Organizations com várias contas e exigir supervisão centralizada de licenças de uma conta de gerenciamento ou de administrador delegado.
- Monitoramento automatizado de conformidade — Quando você precisa de notificações proativas de expiração de licenças e rastreamento automatizado de conformidade em todo o seu AWS ambiente.
- Preparação da auditoria — Quando você precisa de relatórios abrangentes de uso de licenças em toda a organização para auditorias de fornecedores ou análises internas de conformidade.

Comece a usar o License Manager

Para usar AWS License Manager, você deve primeiro concluir as etapas de integração. O procedimento a seguir orienta você pelas etapas de integração no Console de gerenciamento da AWS.

Comece a usar o License Manager

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Você precisará configurar as permissões para o License Manager e seus serviços compatíveis. Siga as instruções para configurar as permissões necessárias.
3. Depois que a configuração inicial for concluída, você pode começar a usar o License Manager para o Casos de uso do License Manager que quiser.

Para obter mais informações sobre como gerenciar permissões para usuários, grupos e funções utilizarem o License Manager e, ao mesmo tempo, seguir as AWS melhores práticas, consulteGerenciamento de identidade e acesso para License Manager. Para obter mais informações sobre como configurar seus EC2 recursos da Amazon que se integram ao License Manager, consulte Configurar para usar a Amazon EC2 no Guia do usuário do Amazon Elastic Compute Cloud.

Trabalhar com o License Manager

O License Manager pode ser aplicado a cenários padrão de empresas com infraestrutura mista de atributos de AWS e atributos on-premises. É possível criar licenças autogerenciadas, fazer inventário dos atributos que consomem licença, associar licenças autogerenciadas a atributos e controlar o inventário e a conformidade.

Licenciamento de produtos AWS Marketplace

Usando o License Manager, agora você pode associar regras de licenciamento aos produtos AWS Marketplace BYOL AMI por meio de modelos de lançamento AWS CloudFormation , modelos ou produtos do Service Catalog do Amazon EC2. Em cada caso, você se beneficia do controle centralizado de licenças e da aplicação de compatibilidade.

> **Note**
>
> O License Manager não altera a forma como você obtém e ativa seu BYOL AMIs no Marketplace. Após o lançamento, você deve fornecer uma chave de licença obtida diretamente do vendedor para ativar qualquer software de terceiros.

Controle de licenças para atributos em datacenters locais

Com o License Manager, você pode descobrir aplicativos executados fora do AWS inventário do Systems Manager e, em seguida, anexar regras de licenciamento a eles. Depois que as regras de licenciamento forem anexadas, você poderá rastrear os servidores on-premises juntamente com os atributos da AWS no console do License Manager.

Diferencie entre licença incluída e BYOL

Com o License Manager, você pode identificar quais atributos têm uma licença incluída no produto e quais usam uma licença pertencente a você. Isso permite relatar com precisão como está usando as licenças BYOL. Esse filtro requer SSM versão 2.3.722.0 ou posterior.

License Manager em todas AWS as suas contas

O License Manager permite que você gerencie licenças em todas as suas AWS contas. Você pode criar configurações de licença uma vez em sua conta AWS Organizations de gerenciamento e compartilhá-las entre suas contas usando AWS Resource Access Manager ou vinculando AWS

Organizations contas usando as configurações do License Manager. Isso também permite que você realize a descoberta de várias contas para pesquisar inventário em suas AWS contas.

Conteúdo

Grupos de ativos de licença

Os grupos de ativos de licenças fornecem uma forma centralizada de gerenciar e monitorar o uso de licenças em todo o seu AWS ambiente. Você pode agrupar ativos relacionados, aplicar regras de licenciamento e monitorar a conformidade em uma conta de gerenciamento ou conta de administrador delegado.

Conteúdo

Compreendendo os grupos de ativos de AWS licenças do License Manager

Os grupos de ativos de licenças AWS License Manager fornecem gerenciamento centralizado de licenças em todas AWS as regiões e contas de uma organização, oferecendo visibilidade

consolidada, notificações automatizadas e relatórios abrangentes para conformidade com licenças de software.

O que são grupos de ativos de licença

Um grupo de ativos de licença é um contêiner AWS License Manager que consolida as licenças e suas EC2 instâncias associadas com base em regras definidas pelo usuário. Esses grupos fornecem uma visão unificada do seu estado de licenciamento de software em todas as suas AWS Organizações, independentemente das regiões ou contas em que as licenças e instâncias residem.

Os grupos de ativos de licenças funcionam aplicando conjuntos de regras que definem quais licenças e instâncias pertencem uma à outra. Por exemplo, você pode criar um grupo de ativos de licença “Windows Server” que rastreie todas as licenças do Windows Server e as EC2 instâncias que executam o Windows Server em sua organização. O grupo descobre e inclui automaticamente os recursos relevantes com base nas regras que você configura.

O sistema oferece suporte a conjuntos AWS de regras gerenciados para produtos de software comuns, como Microsoft Windows Server, SQL Server, Red Hat Enterprise Linux, Ubuntu Pro e SUSE Enterprise Linux, bem como conjuntos de regras personalizados que você pode criar para suas necessidades específicas de licenciamento.

Principais capacidades e componentes

Visibilidade centralizada da licença

Os grupos de ativos de licença agregam informações de licenciamento de várias AWS regiões em uma única visualização. Essa visibilidade entre regiões elimina a necessidade de verificar cada região individualmente para entender o estado de licenciamento de software da sua organização. Os grupos descobrem automaticamente os produtos de software em execução em suas cargas de trabalho usando o AWS Systems Manager agente e consolidam essas informações para obter visibilidade em toda a organização.

Organização flexível baseada em regras

Os grupos de ativos de licenças usam conjuntos de regras para definir quais licenças e instâncias eles rastreiam e mantêm. Esse relacionamento flexível entre grupos e conjuntos de regras permite que você organize suas licenças de forma que atenda às suas necessidades comerciais. Você pode usar conjuntos AWS de regras gerenciados para produtos amplamente adotados ou criar regras personalizadas para software especializado.

Monitoramento automatizado de conformidade

Grupos de ativos de licença fornecem notificações automáticas de expiração de licenças por meio do Amazon SNS, ajudando você a gerenciar proativamente as renovações de licenças. O consumo de licenças é monitorado em relação às dimensões de uso definidas, como vCPU, soquetes, instância ou métricas principais, garantindo que você mantenha o conhecimento de suas obrigações de licenciamento.

Integração com AWS serviços existentes

Os grupos de ativos de licenças se baseiam nos AWS License Manager recursos existentes e se integram a vários AWS serviços para fornecer gerenciamento abrangente de licenças. O recurso funciona junto com as configurações de licença e os recursos de descoberta automatizada que você talvez já esteja usando.

Para permitir a descoberta de software, instale o AWS Systems Manager agente em suas EC2 instâncias. Para cenários com várias contas, você precisa configurar a descoberta entre contas e garantir as permissões apropriadas do IAM para as operações do License Manager em toda a organização.

Introdução aos grupos de ativos de licenças

Esta seção ajuda você a começar a usar grupos de ativos de licença em AWS License Manager. Você aprenderá a configurar os pré-requisitos, configurar regiões de origem e criar seu primeiro grupo de ativos de licença.

Pré-requisitos

Antes de começar a usar grupos de ativos de licença, verifique se você tem os seguintes pré-requisitos:

- AWS Systems Manager Agente (SSM) instalado em suas instâncias EC2
- Detecção entre contas configurada para gerenciar licenças em várias contas
- Se você estiver se integrando pela primeira vez, siga o guia de introdução do License Manager para configurar todas as permissões necessárias

Configurar grupos de ativos de licença

Configurar regiões de origem

Os grupos de ativos de licença estão disponíveis em todas as regiões AWS comerciais em AWS License Manager que estão disponíveis. A descoberta entre regiões exige a seleção de AWS regiões de origem durante a configuração. Isso permite que o License Manager descubra todos os softwares nas regiões selecionadas.

Para configurar regiões de origem usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Configurações e, em seguida, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Descoberta de ativos de licença, escolha Editar.
4. Em Descoberta de regiões, selecione as regiões de onde você deseja descobrir seus produtos.
5. Se você for proprietário de uma organização e quiser descobrir em todas as contas da organização, escolha Habilitar.
6. Escolha Salvar alterações.

Trabalhando com grupos de ativos de licenças

Esta seção descreve como criar, atualizar, excluir e gerenciar grupos de ativos de licença no AWS License Manager. Os grupos de ativos de licenças ajudam a rastrear e gerenciar licenças em seus AWS recursos.

Criação de grupos de ativos de licença

Os grupos de ativos de licenças rastreiam e gerenciam licenças em seus AWS recursos. Você pode criar vários grupos de ativos para organizar diferentes produtos de software e modificar suas configurações a qualquer momento para se adaptar às suas necessidades de licenciamento.

> **Note**
>
> Você pode usar um modelo de um clique para criar rapidamente um grupo de ativos de licença ou seguir as etapas abaixo para criar manualmente um grupo de ativos de licença

adicionando vários conjuntos de regras de licença com base em suas necessidades específicas.

Para criar grupos de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Descoberta de ativos de licenças, certifique-se de que a descoberta de regiões seja preenchida com regiões.
4. Na seção Conjunto de regras de ativos de licença, selecione conjuntos de regras AWS gerenciados (regras predefinidas configuradas para produtos gerenciados específicos) ou conjuntos de regras AWS personalizados. Consulte ???.
5. Escolha Criar grupo de ativos de licença com conjunto de regras.
6. Em Nome do grupo de ativos de licença, insira um nome amigável para lembrar como você está agrupando os ativos.
7. (Opcional) Em Descrição do grupo de ativos de licença, insira uma descrição detalhada sobre como você está agrupando os ativos.
8. Em Dimensão de uso, escolha uma das seguintes opções: vCPU, soquetes, instância ou núcleo. Esse campo determina o cálculo de uso dos ativos.
9. Selecione um ou mais conjuntos de regras de ativos de licença, seja Criar novo conjunto de regras ou Adicionar do conjunto de regras AWS gerenciado ou personalizado existente. Consulte ???.
10. (Opcional) Para Tags, adicione uma ou mais tags.
11. Escolha Criar grupo de ativos de licença.

> **Note**
>
> Depois que um grupo de ativos de licença é criado, a descoberta começa automaticamente e normalmente é concluída em 24 horas. Durante esse período, o License Manager verifica suas regiões e contas configuradas para identificar todas as instâncias que correspondem aos critérios do seu conjunto de regras.

Para criar grupos de ativos de licença usando a CLI

- Use o comando `create-license-asset-group`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager create-license-asset-group \
    --name "Windows Server Group" \
    --description "License asset group for Windows Server instances" \
    --license-asset-group-configurations UsageDimension=vCPU \
    --associated-license-asset-ruleset-arns arn:aws:license-
manager:region:account:ruleset/ruleset-id \
    --client-token unique-token
```

Atualização de grupos de ativos de licença

Você pode atualizar grupos de ativos de licença para modificar suas configurações, adicionar ou remover conjuntos de regras e atualizar tags.

Para atualizar grupos de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças.
3. Na seção Grupo de ativos de licença, verifique se um ou mais grupos de ativos de licença estão disponíveis.
4. Para selecionar um grupo de ativos de licença para edição, marque a caixa de seleção e escolha Ações, Editar. Como alternativa, escolha o item em si.
5. Escolha o botão Editar na página do grupo de ativos de licença. A partir daqui, você pode:
   - Edite o nome do grupo de ativos de licença
   - Edite a descrição do grupo de ativos de licença
   - Adicionar ou remover conjuntos de regras de ativos de licença
   - Adicionar ou remover tags de grupos de ativos de licença
6. Escolha Salvar alterações quando suas alterações estiverem concluídas.

Para atualizar grupos de ativos de licença usando a CLI

- Use o comando `update-license-asset-group`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager update-license-asset-group \
    --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-group/group-id \
    --name "Updated Windows Server Group" \
    --description "Updated description for Windows Server instances"
```

Excluindo grupos de ativos de licença

Você pode excluir grupos de ativos de licença que não são mais necessários. Observe que essa ação não pode ser desfeita e os conjuntos de regras associados ao grupo de ativos de licença não serão excluídos.

Para excluir grupos de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças.
3. Na seção Grupo de ativos de licença, verifique se um ou mais grupos de ativos de licença estão disponíveis.
4. Para selecionar um grupo de ativos de licença para exclusão, marque a caixa de seleção e escolha Ações, Excluir. Como alternativa, escolha o item em si e escolha o botão Excluir na página do grupo de ativos de licença.
5. Para excluir permanentemente o grupo de ativos de licença, digite **`confirm`** na caixa de texto e escolha Excluir.

> **Important**
>
> Esta ação não pode ser desfeita. Os conjuntos de regras associados a esse grupo de ativos de licença não serão excluídos.

Para excluir grupos de ativos de licença usando a CLI

- Use o comando `delete-license-asset-group`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager delete-license-asset-group \
    --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-group/group-id
```

Visualizando detalhes do grupo de ativos de licença

Você pode visualizar informações detalhadas sobre seus grupos de ativos de licença, incluindo conjuntos de regras, instâncias e licenças associados.

Para visualizar detalhes do grupo de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças.
3. Na seção Grupo de ativos de licença, verifique se um ou mais grupos de ativos de licença estão disponíveis.
4. Para ver os detalhes de um grupo de ativos de licença, marque a caixa de seleção e escolha Ações, Exibir detalhes. Como alternativa, escolha o item em si.

Para visualizar grupos de ativos de licença usando a CLI

- Use o comando `get-license-asset-group`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager get-license-asset-group \
    --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-group/group-id
```

Listar grupos de ativos de licença

Você pode listar todos os grupos de ativos de licença em sua conta para ver seu status e configuração.

Para listar grupos de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, escolha Grupos de ativos de licença.
3. Veja a lista de grupos de ativos de licença com seus nomes, status e conjuntos de regras associados.

Para listar grupos de ativos de licença usando a CLI

- Use o comando `list-license-asset-groups`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager list-license-asset-groups \
    --max-results 50 \
    --next-token token-from-previous-call
```

Listando ativos descobertos para um grupo de ativos de licença

São necessárias até 24 horas para visualizar todas as instâncias, licenças concedidas e licenças autogerenciadas associadas a um grupo de ativos de licenças. Quaisquer alterações em suas instâncias, licenças concedidas e licenças autogerenciadas são refletidas em 24 horas.

Para listar ativos para um grupo de ativos de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças.
3. Visualize os detalhes de um grupo de ativos de licença marcando a caixa de seleção e escolhendo Ações, Exibir detalhes. Como alternativa, escolha o item em si.
4. Na página do grupo de ativos de licença, você pode ver todas as instâncias, licenças concedidas e licenças autogerenciadas associadas ao grupo de ativos de licença.

Para listar ativos para grupos de ativos de licença usando a CLI

- Use o comando `list-assets-for-license-asset-group`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager list-assets-for-license-asset-group \
    --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-group/group-id
```

Trabalhando com conjuntos de regras de ativos de licença

Esta seção descreve como criar, atualizar, excluir e gerenciar conjuntos de regras de ativos de licença em. AWS License Manager Os conjuntos de regras de ativos de licença definem os critérios de descoberta de recursos para grupos de ativos de licença.

Entendendo os conjuntos de regras

Um conjunto de regras é um recurso dentro do License Manager que define os critérios de descoberta de recursos para um produto. Ele serve como um agrupamento lógico de regras relacionadas que podem ser usadas para descoberta de produtos, com conjuntos de regras que podem ser usados em diferentes produtos.

Há dois tipos diferentes de conjuntos de regras:

- AWS Conjuntos de regras gerenciados - criados e mantidos pelo serviço License Manager
- Conjuntos de regras personalizados - criados e gerenciados por clientes

O principal benefício dos conjuntos de regras é que novas regras podem ser adicionadas a um conjunto de regras, e essas alterações são refletidas automaticamente em todos os grupos de ativos de licenças usando o mesmo conjunto de regras, que é usado automaticamente para descobrir produtos.

Tipos de conjunto de regras

Baseado em licença

Para licenças autogerenciadas ou concedidas, incluindo produtos do Marketplace AWS

Baseado em instâncias

Para descobrir instâncias com base em determinadas propriedades

Cada conjunto de regras contém até 5 regras que definem como descobrir e rastrear seu software. Você pode criar regras para identificar licenças, instâncias ou ambas e combinar várias condições usando AND, OR ou lógica de correspondência exata para direcionar com precisão os recursos que você deseja gerenciar.

A tabela a seguir mostra as chaves disponíveis que você pode usar ao criar regras de conjunto de regras de ativos de licença:

Chaves de regras do conjunto de regras do ativo de licença

Tipo de regra	Chave	Operador	Tipo de valor	Valores aceitos
Licença autogeren ciada	ARN de configuração da licença	Iguais, não iguais	Lista	ARN válido
	AWS ID da conta	Iguais, não iguais	Lista	String
Licença concedida	ARN da licença	Iguais, não iguais	Lista	ARN válido
	SKU do produto	Iguais, não iguais	Lista	String
	Emissor	Iguais, não iguais	Lista	String

Tipo de regra	Chave	Operador	Tipo de valor	Valores aceitos
	Beneficiário	Iguais, não iguais	Lista	String
	Status da licença	Iguais, não iguais	Lista	Status de licença válido
	Região inicial	Iguais, não iguais	Lista	AWS Região válida
Instância	Plataforma	Iguais, não iguais	Lista	Windows, Linux
	EC2 Produto de cobrança	Iguais, não iguais	Lista	windows-server-enterprise, windows-byol,,, rhel, rhel-byol sql-server-standard sql-server-enterprise, ubuntu-pro, suse-linux rhel-high-availability
	Código de produto do Marketplace	Iguais, não iguais	Lista	String
	ID DA AMI	Iguais, não iguais	Lista	String
	Tipo de instância	Iguais, não iguais	Lista	String

Tipo de regra	Chave	Operador	Tipo de valor	Valores aceitos
	ID da instância	Iguais, não iguais	Lista	String
	ID do host	Iguais, não iguais	Lista	String
	AWS ID da conta	Iguais, não iguais	Lista	String

Usando conjuntos AWS de regras gerenciados

AWS fornece conjuntos de regras pré-configurados para produtos de software comuns. Esses conjuntos de regras gerenciados são atualizados e mantidos automaticamente pelo. AWS

Para usar conjuntos AWS de regras gerenciados

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Conjunto de regras de ativos de licença, selecione AWS-conjuntos de regras gerenciados.
4. Navegue pelos conjuntos de regras gerenciados disponíveis e selecione aqueles que correspondem aos seus produtos de software.

Os conjuntos AWS de regras gerenciadas disponíveis incluem:

- Centro de dados do Microsoft Windows Server
- Microsoft SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition
- Red Hat Enterprise Linux
- Ubuntu Pro

- SUSE Enterprise Linux

Criação de conjuntos de regras personalizados

Você pode criar seu próprio conjunto de regras para definir regras de rastreamento de licenças e instâncias que sejam específicas para seu ambiente e seus requisitos.

Para criar conjuntos de regras usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Conjunto de regras do ativo de licença, escolha Criar conjunto de regras.
4. Em Nome do conjunto de regras, insira um nome amigável para o conjunto de regras.
5. Para a descrição do conjunto de regras, forneça uma descrição do que o conjunto de regras deve ser.
6. (Opcional) Adicione tags ao conjunto de regras e escolha Avançar.
7. Na etapa 2 (Configurar a descoberta de licenças), você pode adicionar regras relacionadas às suas licenças. Isso garante que o sistema possa usar a licença para calcular o uso da licença nas instâncias em que o produto está instalado. Embora a configuração da descoberta de licenças seja opcional, recomendamos adicioná-la se você quiser cálculos de uso da licença.
   - Você pode adicionar licenças autogerenciadas e fornecer ARN ou ID da conta
   - Você também pode adicionar licenças concedidas (licenças adquiridas no Marketplace AWS) ARN, ProductSku etc.
   - Você pode adicionar várias regras escolhendo Adicionar regra.
8. Na etapa 3 (Configurar a descoberta de instâncias), você pode adicionar regras sobre como descobrir várias instâncias. Isso garante que as instâncias possam ser encontradas com base nos critérios de seleção e que essas instâncias sejam contabilizadas para o produto em que você está configurando seu grupo de ativos de licença. Você pode adicionar uma ou mais regras selecionando os seguintes campos:
   - Plataforma (Windows ou Linux)
   - EC2 código do produto de cobrança
   - Código do produto Marketplace
   - ID da AMI, ID do host, ID da instância etc.

9. Revise sua configuração e escolha Enviar.
10. Você pode ver seu conjunto de regras criado recentemente em Meus conjuntos de regras.

Para criar conjuntos de regras usando a CLI

- Use o comando `create-license-asset-ruleset`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager create-license-asset-ruleset \
    --name "Custom Windows Ruleset" \
    --description "Custom ruleset for Windows Server tracking" \
    --rules '[
      {
        "RuleStatement": {
          "InstanceRuleStatement": {
            "MatchingRuleStatement": {
              "Attribute": "Platform",
              "Values": ["Windows"]
            }
          }
        }
      }
    ]' \
    --client-token unique-token
```

Atualizando conjuntos de regras

Você pode atualizar conjuntos de regras personalizados para modificar sua configuração, adicionar ou remover regras e atualizar tags.

Para atualizar conjuntos de regras usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Conjunto de regras do ativo de licença, navegue até Meus conjuntos de regras.

4. Para selecionar um conjunto de regras, marque a caixa de seleção associada e escolha Ações, Editar. Como alternativa, escolha o nome do conjunto de regras e escolha o botão Editar na página do conjunto de regras.
5. A partir daqui, você pode fazer as seguintes atualizações:
   - Edite o nome do conjunto de regras
   - Edite a descrição do conjunto de regras
   - Adicionar ou remover tags associadas ao recurso
6. Escolha Avançar quando suas alterações estiverem concluídas. Na próxima tela, você pode:
   - Adicionar ou remover regras
   - Atualize os tipos de licença para as regras existentes
   - Atualize as condições das regras existentes
7. Escolha Avançar quando suas alterações estiverem concluídas. Na próxima tela, você pode:
   - Adicione ou remova regras de inclusão para especificar condições para identificar as instâncias que você deseja incluir
8. Revise e edite as alterações feitas nas telas anteriores. Escolha Enviar para finalizar as alterações.

Para atualizar conjuntos de regras usando a CLI

- Use o comando `update-license-asset-ruleset`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager update-license-asset-ruleset \
    --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/
ruleset-id \
    --name "Updated Custom Windows Ruleset" \
    --description "Updated description for Windows Server tracking"
```

Excluindo conjuntos de regras

Você pode excluir conjuntos de regras personalizados que não são mais necessários. Observe que os conjuntos de regras não podem ser excluídos até serem removidos de todos os grupos de ativos de licença.

Para excluir conjuntos de regras usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Descoberta de ativos de licença e conjunto de regras.
3. Na seção Conjunto de regras do ativo de licença, navegue até Meus conjuntos de regras.
4. Para selecionar um conjunto de regras para exclusão, marque a caixa de seleção associada e escolha Ações, Excluir. Como alternativa, escolha o nome do conjunto de regras e escolha o botão Excluir na página do conjunto de regras.
5. Para excluir permanentemente o conjunto de regras, digite **`confirm`** na caixa de texto e escolha Excluir.

> **Important**
>
> Esta ação não pode ser desfeita. Os conjuntos de regras não podem ser excluídos até serem removidos de todos os grupos de ativos de licença.

Para excluir conjuntos de regras usando a CLI

- Use o comando `delete-license-asset-ruleset`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager delete-license-asset-ruleset \
    --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/
ruleset-id
```

Obtendo detalhes do conjunto de regras

Você pode recuperar informações detalhadas sobre um conjunto de regras específico, incluindo sua configuração e regras.

Para obter conjuntos de regras usando a CLI

- Use o comando `get-license-asset-ruleset`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager get-license-asset-ruleset \
    --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/
ruleset-id
```

Listando conjuntos de regras

Você pode listar todos os conjuntos de regras em sua conta para ter uma visão geral dos conjuntos de regras disponíveis.

Para listar conjuntos de regras usando a CLI

- Use o comando `list-license-asset-rulesets`. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

```
aws license-manager list-license-asset-rulesets \
    --max-results 50 \
    --next-token token-from-previous-call
```

Licenças autogerenciadas no License Manager

As licenças autogerenciadas (anteriormente conhecidas como configurações de licenças) são o núcleo do License Manager. As licenças autogerenciadas contêm regras de licenciamento com base nos termos de seus contratos empresariais. As regras que você cria determinam como AWS

processa os comandos que consomem licenças. Ao criar licenças autogerenciadas, trabalhe em conjunto com a equipe de compliance da sua organização para analisar seus contratos empresariais.

As licenças autogerenciadas podem ser usadas de forma independente em uma única Conta da AWS ou cruzadas Conta da AWS ou integradas a grupos de ativos de licenças para gerenciamento centralizado em várias AWS contas e regiões em toda a organização. AWS Essa integração fornece controle aprimorado e controle de conformidade para ambientes corporativos.

Serviços da AWS como o License Manager, têm cotas de serviço que definem o número máximo de recursos ou operações por região que estão disponíveis para você Conta da AWS para esse serviço. Por exemplo, com o License Manager, você pode ter um máximo de licenças `10` autogerenciadas por recurso, sem mais do que o total de licenças `25` autogerenciadas em qualquer uma delas. Região da AWS Para saber mais sobre as cotas do License Manager, consulte Cotas AWS License Manager de serviço no. Referência geral da AWS

> **Note**
>
> As instâncias gerenciadas do Systems Manager devem estar associadas às licenças autogerenciadas por vCPU e tipo de instância.

Conteúdo

Parâmetros e regras de licença autogerenciados no License Manager

Uma licença autogerenciada consiste em parâmetros básicos e regras que variam de acordo com os valores de parâmetro. Você também pode adicionar tags a licenças autogerenciadas. Depois de criar

uma licença autogerenciada, um administrador pode modificar o número de licenças e o limite de uso para refletir as mudanças nas necessidades de atributos.

Para organizações que gerenciam licenças em várias AWS contas, considere usar grupos de ativos de licenças que fornecem governança centralizada e aplicação de políticas. As licenças autogerenciadas funcionam em contas individuais e podem ser integradas a grupos de ativos de licenças para visibilidade em toda a organização.

Os parâmetros e as regras disponíveis incluem o seguinte:

- Nome da licença autogerenciada — O nome da licença autogerenciada.
- (Opcional) Descrição — Uma descrição da licença autogerenciada.
- Tipo de licença — A métrica usada para contas licenças. Os valores suportados são v CPUs, núcleos, soquetes e instâncias.
- (Opcional) Número de <opção>: o número de licenças usadas por um atributo.
- Status — Indica se a configuração está ativa.
- (Opcional) Data de expiração — Indica quando essa configuração de licença expirará. O cliente pode inserir essa data com base na data de expiração dos termos de suas licenças BYOL.
- Informações do produto — Os nomes e versões dos produtos para descoberta automatizada. Os produtos compatíveis são Windows Server, SQL Server, Amazon RDS for Oracle e Amazon RDS for Db2.
- (Opcional) Regras: elas incluem o seguinte. As regras disponíveis variam de acordo com o tipo de contagem.
  - Afinidade da licença com o host (em dias) — Restringe o uso da licença para o host pelo número especificado de dias. O intervalo é de 1 a 180. O tipo de contagem deve ser Núcleos ou Soquetes. Após o término do período de afinidade, a licença estará disponível para reutilização em 24 horas.
  - Máximo de núcleos — Contagem máxima de núcleos para um atributo.
  - Máximo de soquetes — Contagem máxima de soquetes para um atributo.
  - Máximo v CPUs — Contagem máxima v CPUs para um recurso.
  - Mínimo de núcleos — Contagem mínima de núcleos para um atributo.
  - Mínimo de soquetes — Contagem mínima de soquetes para um atributo.
  - Mínimo v CPUs — Contagem mínima v CPUs para um recurso.
  - Locação — Restringe o uso da licença à locação do EC2 especificada. Hosts Dedicados são necessários se o tipo de contagem for Núcleos ou Soquetes. Locação compartilhada, hosts

dedicados e instâncias dedicadas são compatíveis se o tipo de contagem for Instâncias ou v. CPUs Os nomes do console (e da API) são os seguintes:

- Compartilhado (`EC2-Default`)
- Instância Dedicada (`EC2-DedicatedInstance`)
- Host Dedicado (`EC2-DedicatedHost`)
- Otimização de vCPU — O License Manager se integra ao suporte de otimização de CPU no Amazon EC2, o que permite que você personalize o número de v em uma instância. CPUs Se essa regra for definida como True, o License Manager contará v CPUs com base na contagem personalizada de núcleos e segmentos. Caso contrário, o License Manager conta o número padrão de v CPUs para o tipo de instância.

- Incluir instâncias interrompidas — Quando essa regra é definida como True, o License Manager rastreia as instâncias paradas e as conta como uso da licença. O valor padrão é False. Quando definidas como False, as instâncias interrompidas não são contabilizadas para o uso da licença e suas licenças são liberadas de volta para o pool de licenças disponíveis.

A tabela a seguir descreve quais regras de licença estão disponíveis para cada tipo de contagem.

Nome do console	Nome da API	Núcleos	Instâncias	Soquetes	v CPUs
Afinidade de licença com o host (em dias)	`licenseAffinityToHost`	✓		✓	
Máximo de núcleos	`maximumCores`	✓	✓		
Máximo de soquetes	`maximumSockets`		✓	✓	
Máximo v CPUs	`maximumVcpus`		✓		✓
Mínimo de núcleos	`minimumCores`	✓	✓		
Mínimo de soquetes	`minimumSockets`		✓	✓	
v mínimo CPUs	`minimumVcpus`		✓		✓
Locação	`allowedTenancy`	✓	✓	✓	✓

Nome do console	Nome da API	Núcleos	Instâncias	Soquetes	v CPUs
Otimização de vCPU	`honorVcpuOptimization`				✓
Incluir instâncias interrompidas	`includedStoppedInstances`	✓	✓	✓	✓

Como criar regras do License Manager a partir de licenças de fornecedores

Você pode criar conjuntos de regras do License Manager com base na linguagem das licenças dos fornecedores de software. Os exemplos a seguir não são esquemas para casos de uso reais. Em qualquer aplicação real de um contrato de licença, você escolhe entre opções concorrentes, dependendo da arquitetura e do histórico de licenciamento do seu ambiente de servidor on-premises específico. Suas opções também dependem dos detalhes da migração planejada de atributos para o AWS.

Sempre que possível, esses exemplos devem ser neutros em relação a fornecedores, concentrando-se em questões de alocação de hardware e software que podem ser aplicadas de forma geral. As disposições de licenciamento do fornecedor também interagem com AWS os requisitos e limites. O número de licenças necessárias para um aplicativo varia de acordo com o tipo de instância escolhido e outros fatores.

> **Important**
>
> AWS não participa do processo de auditoria com fornecedores de software. Os clientes são responsáveis pela compatibilidade e assumem a responsabilidade de compreender e capturar com cuidado as regras do License Manager com base nos contratos de licenciamento.

Exemplo: implementação de uma licença de sistema operacional

Este exemplo envolve uma licença para um sistema operacional de servidor. A linguagem de licenciamento impõe restrições ao tipo de núcleo da CPU, locação e número mínimo de licenças por servidor.

Neste exemplo, os termos de licenciamento incluem as seguintes estipulações:

- Núcleos do processador físico determinam a contagem de licenças.
- O número de licenças deve ser igual ao número de núcleos.
- Um servidor deve executar no mínimo oito núcleos.
- O sistema operacional deve ser executado em um host não virtualizado.
- As licenças devem permanecer alocadas mesmo quando as instâncias são interrompidas.

Além disso, o cliente tomou as seguintes decisões:

- Licenças para 96 núcleos foram compradas.
- Um limite rígido é imposto para restringir o consumo de licenças à quantidade comprada.
- Cada servidor precisa de um máximo de 16 núcleos.

A tabela abaixo associa os parâmetros de criação de regras do License Manager aos requisitos de licenciamento de fornecedores que eles capturam e automatizam. Os valores de exemplo são apenas para fins ilustrativos. Você precisa especificar os valores necessários nas suas próprias licenças autogerenciadas.

Regra do License Manager	Configurações
Tipo de contagem de licenças	Tipo de licença é definido como **`Cores`**.
Contagem de licenças	Número de núcleos é definido como **`96`**.
V mínimo/máximo CPUs para núcleos	Mínimo de núcleos é definido como **`8`**. Máximo de núcleos é definido como **`16`**.
Limite rígido de contagem de licenças	Aplicar limite de licença está selecionado.
Locação permitida	Locação está definida como **`Dedicated Host`**.

Regra do License Manager	Configurações
Incluir instâncias interrompidas	A opção Incluir instâncias interrompidas está definida como**`True`**. As instâncias interrompidas continuam consumindo licenças.

Crie uma licença autogerenciada no License Manager

Uma licença autogerenciada representa os termos de licenciamento no contrato com seu fornecedor de software. Sua licença autogerenciada especifica como suas licenças devem ser contadas (por exemplo, por v CPUs ou número de instâncias). Ela também especifica limites que previnem que o uso ultrapasse o número de licenças alocadas. Além disso, as licenças autogerenciadas também podem especificar outras restrições, como o tipo de locação.

> **Note**
>
> Antes de criar uma licença autogerenciada, considere sua estrutura organizacional:
>
> - Uso de conta única: crie licenças autogerenciadas diretamente na sua conta
> - Uso de várias contas: considere primeiro criar grupos de ativos de licenças e, em seguida, associar licenças autogerenciadas para gerenciamento centralizado

Considerações sobre o Amazon RDS for Oracle e o Amazon RDS para bancos de dados Db2

Quando você adiciona informações do produto para configurar a descoberta automática dos bancos de dados Amazon RDS for Oracle ou Amazon RDS for Db2, os seguintes requisitos se aplicam:

- O tipo de contagem de licenças compatível é `vCPU`.
- Não há suporte para regras.
- Não há suporte para limites rígidos de licenças.
- Você pode monitorar uma versão do produto por licença autogerenciada.
- Você não pode rastrear bancos de dados do Amazon RDS e outros produtos usando a mesma licença autogerenciada.

Para criar uma licença autogerenciada usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha Criar licença autogerenciada.
4. No painel Detalhes da configuração, forneça as seguintes informações:

   - Nome da licença autogerenciada — O nome da licença autogerenciada.
   - Descrição — Uma descrição opcional da licença autogerenciada.
   - Data de expiração — Uma data de expiração opcional da licença autogerenciada.
   - Tipo de licença — O modelo de contagem dessa licença (v CPUs, núcleos, soquetes ou instâncias).
   - Número de <opção>: a opção exibida depende do tipo de licença. Quando o limite de licenças for excedido, o License Manager notificará você (limite flexível) ou impedirá a implantação de um atributo (limite rígido).
   - Aplicar limite de licença — Quando selecionado, o limite será rígido.
   - Regras — Uma ou mais regras. Para cada regra, selecione um tipo, forneça um valor e escolha Adicionar regra. Os tipos de regra exibidos dependem do tipo de licença. Por exemplo, valores mínimos, valores máximos e locação. Se você não especificar um tipo de locação, todos serão aceitos.
5. (Opcional) No painel de Regras de descoberta automatizada, faça o seguinte:

   a. Escolha o nome do produto, o tipo de produto e o tipo de atributo para descobrir e rastrear usando a descoberta automatizada.

   b. Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.

   c. (Opcional) Se sua conta for uma conta de gerenciamento do License Manager para uma Organizations, você tem a opção de definir atributos a serem excluídos da descoberta automática. Para fazer isso, selecione Adicionar regra de exclusão, escolha a propriedade para filtrar, as tags de AWS conta IDs e recurso são suportadas e, em seguida, insira as informações para identificar essa propriedade.
6. (Opcional) Expanda o painel Tags para adicionar uma ou mais tags à sua licença autogerenciada. As etiquetas são key/value pares. Forneça as seguintes informações para cada tag:

- Chave - O nome pesquisável da chave.
- Valor - O valor da chave.

7. Selecione Enviar.

> **Note**
>
> Depois que a data de expiração da licença for definida, o License Manager poderá enviar notificações em 120 dias, 90 dias, 60 dias, 30 dias, 0 dias para o tópico do Amazon SNS que está configurado em. Configurações de licença gerenciada no License Manager

Para criar uma licença autogerenciada usando a linha de comando

- create-license-configuration (AWS CLI)
- Nova LICMLicense configuração (Ferramentas da AWS para PowerShell)

Compartilhe uma licença autogerenciada no License Manager

Você pode usar AWS Resource Access Manager para compartilhar suas licenças autogerenciadas com qualquer AWS conta ou por meio de. AWS Organizations Para obter mais informações, consulte Compartilhando seus AWS recursos no Guia AWS RAM do usuário.

Compartilhe uma licença autogerenciada com sua organização AWS

Pré-requisitos

Para concluir esse procedimento, você deve vincular sua AWS organização ao License Manager. Para obter mais informações, consulte Configurações de licença gerenciada no License Manager.

Compartilhe sua licença

Para compartilhar uma licença autogerenciada com sua AWS organização, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Selecione a licença autogerenciada.
4. Escolha Compartilhar com contas da AWS organização no menu Ações.

Cota de contas compatíveis

Se você habilitou o compartilhamento de licenças AWS License Manager antes de 14 de outubro de 2023, sua cota para o número máximo de contas que o License Manager suporta em sua organização será menor do que o novo máximo padrão. Você pode aumentar essa cota usando operações de API, pois AWS RAM elas são fornecidas na seção a seguir. Para obter mais informações sobre as cotas padrão no License Manager, consulte Cotas para trabalhar com licenças no Guia Referência geral da AWS .

Pré-requisitos

Para concluir o procedimento seguinte, você deve fazer login como entidade principal na conta de gerenciamento da organização que tem as seguintes permissões:

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Como aumentar a cota de contas compatíveis

O procedimento a seguir aumentará sua cota atual de `Number of accounts per organization for License Manager` até o atual padrão máximo.

Para aumentar a cota de contas compatíveis no License Manager

1. Use o describe-organization AWS CLI comando para determinar o ARN da sua organização usando a operação:

```
aws organizations describe-organization

{
 "Organization": {
  "Id": "o-abcde12345",
  "Arn": "arn:aws:organizations::111122223333:organization/o-abcde12345",
  "FeatureSet": "ALL",
  "MasterAccountArn": "arn:aws:organizations::111122223333:account/o-
abcde12345/111122223333",
  "MasterAccountId": "111122223333",
  "MasterAccountEmail": "name+orgsidentifier@example.com",
```

```
  "AvailablePolicyTypes": [
    {
     "Type": "SERVICE_CONTROL_POLICY",
     "Status": "ENABLED"
    }
  ]
 }
}
```

2. Use o get-resource-shares AWS CLI comando para determinar o ARN da sua organização usando a operação:

```
aws ram  get-resource-shares --resource-owner SELF --tag-filters
 tagKey=Service,tagValues=LicenseManager --region us-east-1

{
 "resourceShares": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "name": "licenseManagerResourceShare-111122223333",
    "owningAccountId": "111122223333",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "tags": [
     {
      "key": "Service",
      "value": "LicenseManager"
     }
    ],
    "creationTime": "2023-10-04T12:52:10.021000-07:00",
    "lastUpdatedTime": "2023-10-04T12:52:10.021000-07:00",
    "featureSet": "STANDARD"
  }
 ]
}
```

3. Use o enable-sharing-with-aws-organization AWS CLI comando para ativar o compartilhamento de recursos com AWS RAM:

```
aws ram enable-sharing-with-aws-organization

{
```

```
 "returnValue": true
}
```

Você pode usar o list-aws-service-access-for-organization AWS CLI comando para verificar se os diretores de serviço das listas de Organizations estão habilitados para o License Manager e AWS RAM:

```
aws organizations list-aws-service-access-for-organization

{
 "EnabledServicePrincipals": [
  {
    "ServicePrincipal": "license-manager.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.814000-07:00"
  },
  {
    "ServicePrincipal": "license-manager.member-account.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.565000-07:00"
  },
  {
    "ServicePrincipal": "ram.amazonaws.com",
    "DateEnabled": "2023-10-04T13:06:34.771000-07:00"
  }
 ]
}
```

> **Important**
>
> Pode levar até seis horas AWS RAM para concluir essa operação em sua organização. Esse processo precisa estar concluído antes que você possa continuar.

4. Use o associate-resource-share AWS CLI comando para associar seu compartilhamento de recursos do License Manager à sua organização:

```
aws ram associate-resource-share --resource-share-arn arn:aws:ram:us-
east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --
principals arn:aws:organizations::111122223333:organization/o-abcde12345 --
region us-east-1

{
 "resourceShareAssociations": [
```

```
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATING",
    "external": false
  }
 ]
}
```

Você pode usar o get-resource-share-associations AWS CLI comando para validar se a associação de compartilhamento de recursos `status` é`ASSOCIATED`:

```
aws ram get-resource-share-associations --association-type "PRINCIPAL" --principal
 arn:aws:organizations::111122223333:organization/o-abcde12345--resource-share-
arns arn:aws:ram:us-east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "resourceShareName": "licenseManagerResourceShare-111122223333",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATED",
    "creationTime": "2023-10-04T13:12:33.422000-07:00",
    "lastUpdatedTime": "2023-10-04T13:12:34.663000-07:00",
    "external": false
  }
 ]
}
```

Edite uma licença autogerenciada no License Manager

É possível editar os valores dos seguintes campos em uma licença autogerenciada:

- Nome da licença autogerenciada
- Description
- Data de expiração
- Número de <opção>
- Aplicar o limite do tipo de licença
- Incluir instâncias interrompidas

Para editar uma licença autogerenciada

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Selecione a licença autogerenciada.
4. Selecione Ações, Editar.
5. Edite os detalhes conforme necessário e escolha Atualizar.

> **Note**
>
> Depois que a data de expiração da licença for definida, o License Manager poderá enviar notificações em 120 dias, 90 dias, 60 dias, 30 dias, 0 dias para o tópico do Amazon SNS que está configurado em. Configurações de licença gerenciada no License Manager

Para editar uma licença autogerenciada usando a linha de comando

- update-license-configuration (AWS CLI)
- Atualização - LICMLicense Configuração (Ferramentas da AWS para PowerShell)

Visualize licenças autogerenciadas no License Manager

Você pode visualizar suas licenças autogerenciadas por meio do console do License Manager para monitorar o uso, a conformidade e a distribuição em seu AWS ambiente.

Veja as licenças em uma única conta

Para ver as licenças autogerenciadas em sua conta atual:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, selecione **`Self-managed licenses`**.
3. Revise a lista de licenças, seu status e uso atual.
4. Escolha um nome de licença para ver informações detalhadas, incluindo recursos associados e status de conformidade.

Exibir licenças agregadas (para administrador da organização ou administrador delegado)

Administradores da organização e administradores delegados podem visualizar licenças autogerenciadas em todas as AWS contas da organização a partir de um local centralizado. Isso fornece visibilidade e recursos de gerenciamento em toda a organização para conformidade com as licenças.

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Verifique se você está conectado como administrador da organização ou administrador delegado.
3. No painel de navegação à esquerda, selecione **`Self-managed licenses`**.
4. Escolha a **`Organization license configuration`** guia para ver a visualização agregada da licença.
5. Analise a visão agregada de todas as licenças autogerenciadas nas contas da sua organização.

Essa visão agregada permite uma governança centralizada de licenças e ajuda a garantir a conformidade em toda a AWS organização.

Para visualizar licenças agregadas usando a linha de comando

- list-license-configurations-for-organização ()AWS CLI

Desative uma licença autogerenciada no License Manager

Quando você desativa uma licença autogerenciada, os recursos existentes que usam a licença não são afetados e o AMIs uso da licença ainda pode ser iniciado. No entanto, o consumo da licença não é mais rastreado.

Quando uma licença autogerenciada é desativada, ela não deve estar anexada a nenhuma instância em execução. Após a desativação, execuções não poderão ser realizadas com a licença autogerenciada.

Para desativar uma licença autogerenciada

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Selecione a licença autogerenciada.
4. Escolha Ações, Desativar. Quando a confirmação for solicitada, escolha Desativar.

Para desativar uma licença autogerenciada usando a linha de comando

- update-license-configuration (AWS CLI)
- Atualização - LICMLicense Configuração (Ferramentas da AWS para PowerShell)

Excluir uma licença autogerenciada no License Manager

Antes de excluir uma licença autogerenciada, é preciso desassociar todos os atributos. Você pode excluir uma licença autogerenciada se precisar recomeçar com novas regras de licenciamento. Se os termos de licenciamento de seus fornecedores de software mudarem, você poderá desassociar os atributos existentes, excluir a licença autogerenciada, criar uma nova licença autogerenciada para refletir os termos atualizados e associá-la aos atributos existentes.

Para excluir uma licença autogerenciada usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Selecione cada um dos atributos (individualmente ou em lote) e escolha Desassociar atributo. Repita até a lista estar vazia.
5. Escolha Ações, Excluir. Quando a confirmação for solicitada, escolha Excluir.

Para excluir uma licença autogerenciada usando a linha de comando

- delete-license-configuration (AWS CLI)

- Remover- LICMLicense Configuração (Ferramentas da AWS para PowerShell)

Regras de licença autogerenciadas no License Manager

Depois que as regras de licença autogerenciada estiverem em vigor, elas podem ser anexadas aos mecanismos de inicialização relevantes, que podem impedir diretamente a implantação de novos atributos que não sejam compatíveis. Os usuários da sua organização podem iniciar facilmente instâncias do EC2 a partir de instâncias designadas AMIs, e os administradores podem monitorar o inventário de licenças por meio do painel integrado do License Manager. Os controles de execução e os alertas do painel permitem uma aplicação mais fácil da conformidade.

> **Important**
>
> AWS não participa do processo de auditoria com fornecedores de software. Os clientes são responsáveis pela compatibilidade e assumem a responsabilidade de compreender e capturar com cuidado as regras do License Manager com base nos contratos de licenciamento.

O controle de licenças funciona a partir das regras de tempo anexadas a uma instância até seu encerramento. Você define seus limites de uso e regras de licenciamento, e o rastreia implantações e, ao mesmo tempo, alerta você sobre violações de regra. Se você tiver configurado limites rígidos, o License Manager poderá evitar que atributos sejam iniciados.

Quando um servidor rastreado é encerrado, sua licença é liberada e devolvida ao conjunto de licenças disponíveis. Por padrão, quando um servidor rastreado é interrompido, sua licença também é liberada e devolvida ao pool. No entanto, se a regra Incluir instâncias interrompidas (`includedStoppedInstances`) for definida como True, as instâncias interrompidas continuarão sendo rastreadas e contabilizadas como uso da licença. Isso é útil quando seus termos de licenciamento exigem que as licenças permaneçam alocadas às instâncias, independentemente de seu estado de execução.

Como as organizações têm diferentes abordagens para operações e compatibilidade, o License Manager oferece suporte a vários mecanismos de execução:

- Associação manual de licenças autogerenciadas com AMIs — Para rastrear licenças para sistema operacional ou outro software, você pode anexar regras de licenciamento AMIs antes de publicá-las para uso mais amplo em sua organização. Todas as implantações dessas AMIs são então

rastreadas automaticamente com o License Manager sem exigir nenhuma ação adicional dos usuários. Você também pode anexar regras de licenciamento aos seus mecanismos de criação de AMI atuais, como Systems Manager Automation, VM Import/Export e Packer.

- Modelos de lançamento do Amazon EC2 e AWS CloudFormation — Se anexar regras de licenciamento não AMIs for uma opção preferida, você pode especificá-las como parâmetros opcionais nos modelos ou modelos de lançamento do EC2.CloudFormation Implantações com esses modelos são rastreadas usando o License Manager. Você pode aplicar regras em modelos ou CloudFormation modelos de execução do EC2 especificando uma ou mais licenças autogerenciadas IDs no campo de licenças autogerenciadas.

AWS trata os dados de rastreamento de licenças como dados confidenciais do cliente, acessíveis somente por meio da AWS conta proprietária. AWS não tem acesso aos seus dados de rastreamento de licenças. Você controla seus dados de controle de licenças e pode excluí-los a qualquer momento.

Associando licenças autogerenciadas e AMIs

O procedimento a seguir demonstra como associar licenças autogerenciadas ao AMIs uso do console do License Manager. O procedimento pressupõe que você tenha pelo menos uma licença autogerenciada existente. Você pode associar configurações de licença a qualquer AMI a que você tenha acesso, seja de propriedade ou compartilhada. Se uma AMI foi compartilhada com você, poderá associá-la à licença autogerenciada na conta atual. Caso contrário, você pode especificar se a AMI está associada à licença autogerenciada em todas as contas ou somente na conta atual.

Se você associar uma AMI a uma licença autogerenciada em todas as contas, poderá acompanhar as execuções de instâncias da AMI em todas as contas. Quando um limite rígido é atingido, o License Manager bloqueia a execução de instâncias adicionais. Quando um limite suave é atingido, o License Manager notifica sobre a execução de instâncias adicionais.

Se você copiar uma AMI dentro da mesma região e essa AMI tiver configurações de licença associadas, essas configurações de licença serão automaticamente associadas à nova AMI. Quando você executa uma instância a partir da nova AMI, o License Manager a rastreia. Da mesma forma, se você criar uma nova AMI a partir de uma instância em execução que tenha configurações de licença associadas, essas configurações de licença serão automaticamente associadas à nova AMI, e o License Manager rastreará as instâncias que você executa a partir da nova AMI.

> **Warning**
>
> O License Manager não oferece suporte ao rastreamento de instâncias entre regiões. Se você copiar uma AMI que tenha configurações de licença associadas para uma região diferente, o License Manager bloqueia todas as execuções de instância da nova AMI.

Para associar uma licença autogerenciada e uma AMI

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença. Para ver o associado atualmente AMIs, escolha Associado AMIs.
4. Escolha Associar AMI.
5. AMIsEm Disponível, selecione um ou mais AMIs e escolha Associar.
   - Se sua conta possuir pelo menos um deles AMIs, você será solicitado a escolher um escopo de associação de AMI para o AMIs que você possui. Todos os AMIs que foram compartilhados com outra conta são associados somente à sua conta. Escolha Confirmar.
   - Se eles AMIs foram compartilhados com você de outra conta, eles serão associados somente à sua conta.

   Os recém-associados AMIs agora aparecem na AMIs guia Associado na página de detalhes da licença.

Desassociando licenças autogerenciadas e AMIs

O procedimento a seguir demonstra como dissociar licenças autogerenciadas do uso do console do AMIs License Manager. Você não pode desassociar uma AMI com o registro cancelado. O License Manager verifica se há registros cancelados a AMIs cada 8 horas e os desassocia automaticamente.

Para desassociar uma licença autogerenciada e uma AMI

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Escolha Associado AMIs.

5. Selecione o link e escolha Desassociar AMI.

Licenças concedidas no License Manager

Licenças concedidas são licenças para produtos que sua organização comprou no AWS Marketplace, no AWS Data Exchange, ou diretamente de um vendedor que integrou seu software com direitos gerenciados. Os administradores de licenças podem usar AWS License Manager para controlar o uso dessas licenças e distribuir direitos de uso, conhecidos como direitos, para contas específicas. AWS

As licenças de dados distribuídas aos produtos do AWS Data Exchange estão disponíveis para a AWS conta por meio do AWS Data Exchange. Antes de distribuir licenças de AWS Marketplace, você deve habilitar o compartilhamento de assinaturas. Para obter mais informações, consulte Compartilhar assinaturas em uma organização.

Depois que um administrador de licença distribui o direito de uma AWS Marketplace licença para uma AWS conta e o destinatário aceita e ativa a licença concedida, a assinatura fica disponível para a conta por meio de. AWS AWS Marketplace A conta também tem acesso ao produto. Por exemplo, se um administrador de licença comprar uma Amazon Machine Image (AMI) AWS Marketplace e distribuir um direito à sua AWS conta, você pode iniciar EC2 instâncias da Amazon a partir da AMI usando a Amazon. AWS Marketplace EC2

Tópicos

Visualizar suas licenças concedidas

O License Manager possui guias para visualizar e gerenciar suas licenças concedidas com base nas permissões com as quais você está autenticado. A página de licenças concedidas pode exibir as seguintes guias:

Minhas licenças

Essa guia está disponível para qualquer usuário que tenha acesso para visualizar as licenças concedidas no License Manager. A guia tem uma seção Minhas licenças concedidas, que inclui informações como o ID da licença e o nome do produto. Nessa página, você pode ver informações adicionais sobre cada licença.

Resumo da licença (para administradores da organização)

Essa guia está disponível somente para administradores da organização. Ela tem uma seção de Totais, que lista a quantidade total de produtos e licenças concedidas em todas as contas da sua organização. Ela também mostra uma seção Produtos, que inclui uma tabela detalhando propriedades como o Nome do produto e Número de licenças concedidas.

Licenças agregadas (para administradores da organização)

Essa guia está disponível somente para administradores da organização. Ela tem uma seção que detalha as Licenças concedidas à minha organização, que inclui informações como o ID da licença e o Nome do produto. Nessa página, você pode ver informações adicionais sobre cada licença.

Gerencie suas licenças concedidas no License Manager

As licenças que foram concedidas a você aparecerão no console do License Manager. Os destinatários precisam aceitar e ativar as licenças concedidas antes de poderem usar o produto. A forma como você aceita e ativa uma licença depende se a licença é de AWS Marketplace, se sua conta é membro de uma organização e se todos os recursos estão habilitados para sua organização. AWS Organizations

As licenças concedidas exigem a replicação entre Regiões dos metadados da licença. O License Manager replica automaticamente cada licença concedida e suas informações associadas para outras Regiões da AWS. Isso permite que você tenha uma visão centralizada de todas as Regiões em que licenças são concedidas a você.

Licenças AWS Marketplace e AWS Data Exchange

- As licenças das assinaturas que você compra são automaticamente aceitas e ativadas.
- Se a conta de gerenciamento de uma organização com todos os atributos habilitados comprar uma assinatura e distribuir licenças para as contas dos membros, as licenças serão automaticamente

aceitas nessas contas. A conta de gerenciamento ou as contas dos membros podem ativar a licença posteriormente.

- Se a conta de gerenciamento de uma organização com apenas os atributos de faturamento consolidado habilitados comprar uma assinatura e distribuir licenças para as contas dos membros, cada membro precisa aceitar e ativar a licença.

Licenças de um vendedor

- Você precisa aceitar e ativar licenças para produtos que usam o License Manager para distribuir licenças.
- Se a conta de gerenciamento de uma organização com todos os atributos habilitados comprar um produto e distribuir licenças para as contas dos membros, as licenças serão automaticamente aceitas nessas contas. A conta de gerenciamento ou as contas dos membros podem ativar a licença posteriormente.
- Se a conta de gerenciamento de uma organização com apenas os atributos de faturamento consolidado habilitados comprar um produto e distribuir licenças para as contas dos membros, cada membro precisa aceitar e ativar a licença.

Console (My licenses)

Você só pode visualizar e gerenciar as licenças concedidas em uma única conta da Conta da AWS.

Como gerenciar licenças concedidas na sua conta

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças concedidas.
3. Selecione a guia Minhas licenças, se ela não estiver selecionada.
4. (Opcional) Use as opções de filtro, como as mostradas abaixo, para restringir o escopo da lista exibida.

    - SKU do produto — O identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs.
    - Destinatário — O ARN do destinatário da licença.
    - Status — O status da licença. Por exemplo, Disponível.

5. Para ver informações adicionais sobre a licença, escolha o ID correspondente para abrir a página Visão geral da licença.
6. Se o emissor da licença for uma entidade diferente AWS Marketplace, o status inicial da concessão será Aceitação pendente. Execute um destes procedimentos:
   - Escolha Aceitar e ativar a licença. O status de concessão resultante é Ativa.
   - Escolha Aceitar licença. O status de concessão resultante é Desativada. Quando quiser usar a licença, escolha Ativar licença.
   - Escolha Rejeitar licença. O status de concessão resultante é Rejeitada. Depois de rejeitar uma licença, não é possível ativá-la.

Se você quiser parar de usar uma licença que foi ativada, retorne à página Visão geral da licença e escolha Desativar licença. Se você quiser voltar a usar uma licença que foi desativada, retorne à página Visão geral da licença e escolha Ativar licença.

Console (Aggregated licenses)

Você pode ver as licenças concedidas que foram agregadas a partir de todas as contas da organização.

> **Important**
>
> Para usar a visão geral da organização para suas licenças concedidas, você deve primeiro vincular AWS Organizations usando as configurações do AWS License Manager console. Para obter mais informações, consulte Configurações no License Manager.

Para gerenciar as licenças concedidas em suas contas em AWS Organizations

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças concedidas.
3. Selecione a guia Licenças agregadas, se ela não estiver selecionada.
4. (Opcional) Use as opções de filtro, como as mostradas abaixo, para restringir o escopo da lista exibida.
   - SKU do produto — O identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs.
   - Beneficiário — A conta da sua organização à qual a licença foi concedida.

5. Para ver informações adicionais sobre a licença, escolha o ID correspondente para abrir a página “Detalhes da licença”.
6. Se o emissor da licença for uma entidade diferente de AWS Marketplace, faça o seguinte:
   - Escolha Ativar a licença. O status de concessão resultante é Ativa.
   - Escolha Desativar a licença. O status de concessão resultante é Desativada.

Se você quiser parar de usar uma licença que foi ativada, retorne à página Visão geral da licença e escolha Desativar licença. Se você quiser voltar a usar uma licença que foi desativada, retorne à página Visão geral da licença e escolha Ativar licença.

AWS CLI

Você pode usar o AWS CLI para trabalhar com suas licenças concedidas.

Para gerenciar as licenças usando o AWS CLI:

- accept-grant
- create-grant-version
- get-grant
- list-licenses
- list-received-grants
- list-received-grants-for-organization
- list-received-licenses
- list-received-licenses-for-organization
- reject-grant

Distribua direitos do License Manager

Se você for um administrador de licenças operando na conta de gerenciamento da organização com todos os atributos habilitados, você pode distribuir direitos para a organização a partir das licenças concedidas criando uma concessão. Para obter mais informações sobre AWS Organizations, consulte AWS Organizations terminologia e conceitos.

Os destinatários da licença podem ser os seguintes:

- Um Conta da AWS, que inclui somente a conta especificada.

- A raiz de uma organização, o que incluirá todas as contas dela.
- Uma unidade organizacional (OU) (que não está aninhada), que inclui todas as contas na OU especificada e aninhadas na OUs OU especificada.

> **Note**
>
> Você pode criar até 2.000 concessões por licença.

Você pode usar o AWS License Manager console ou o AWS CLI para distribuir seus direitos. Você pode especificar o ID ou o ARN da organização ao criar uma concessão no console, mas o formato ARN deve ser usado com o AWS CLI. Por exemplo, ARNs será semelhante ao seguinte:

ARN do ID da organização

```
arn:aws:organizations::<account-id-of-management-account>:organization/
o-<organization-id>
```

ARN da UO da organização

```
arn:aws:organizations::<account-id-of-management-account>:ou/
o-<organization-id>/ou-<organizational-unit-id>
```

Console

Para criar uma concessão (Console)

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças concedidas.
3. Escolha um ID de licença para abrir a página Visão geral da licença.
4. Na seção Concessões, escolha Criar concessão.
5. Na página Detalhes da concessão, faça o seguinte:
   a. Insira um nome que vai ajudar você a identificar a finalidade ou o destinatário da concessão.
   b. Insira o Conta da AWS ID, AWS Organizations ID da OU ou ARN, ou AWS Organizations ID ou ARN do beneficiário do subsídio.
   c. Escolha Criar concessão.

6. Na página de Visão geral da licença, você verá uma entrada para a concessão no painel Concessões. O status inicial da concessão é Aceitação pendente. O status muda para Ativa quando o destinatário aceita a concessão ou para Rejeitada quando o destinatário a rejeita.

AWS CLI

Você pode usar o AWS CLI para distribuir um direito. Você deve especificar uma ID da organização ou OU no formato ARN ao usar a AWS License Manager API.

Para criar e listar suas concessões usando o AWS CLI:

- create-grant
- list-distributed-grants

A página “Detalhes das concessões” exibe a lista de contas às quais você concedeu acesso ao direito. Depois de distribuir uma licença para sua organização, você pode desativar ou ativar as licenças individualmente em cada conta.

Conceda aceitação e ativação no License Manager

Quando uma concessão é criada para uma licença concedida, ela é distribuída ao destinatário. Uma licença concedida deve ser aceita e ativada antes que possa ser usada pelo destinatário. O processo de ativação da concessão pode incluir opções adicionais para licenças concedidas provenientes do AWS Marketplace.

Por padrão, a página Visão geral da concessão de uma licença concedida tem o status de `Pending Acceptance`. Você pode `Accept`, `Accept and Activate` ou `Reject` a concessão. Concessões aceitas, mas ainda não ativadas, têm o status de `Disabled`. Concessões aceitas e ativadas têm o status de `Active`.

Uma licença concedida deve ser aceita e ativada antes que possa ser usada pelo destinatário. Por padrão, a página “Detalhes da concessão” de uma licença concedida tem o status de Aceitação pendente. Você pode Aceitar, Aceitar e Ativar ou Rejeitar a licença. Concessões aceitas, mas ainda não ativadas, têm o status de Desativadas. Concessões aceitas e ativadas têm o status de Ativas.

> **Tip**
>
> Você pode aceitar automaticamente concessões provenientes da conta de gerenciamento da sua organização. Para ativar a aceitação automática da concessão, vincule as contas da sua

organização na página de configurações no AWS License Manager console a partir da conta de gerenciamento.

Você não pode ativar duas licenças para o mesmo produto AWS Marketplace ao mesmo tempo. Se você tiver duas assinaturas (por exemplo, a oferta pública para um produto e uma oferta privada, ou uma licença assinada para um produto e uma licença concedida para o mesmo produto), você tem as seguintes opções:

1. Desative a concessão existente para o produto e, em seguida, ative a nova concessão.
2. Ative a nova concessão e especifique que você deseja desativar e substituir a concessão existente. Você pode usar o console do License Manager ou o AWS CLI:
   a. Usando o console do License Manager, ative a nova concessão e selecione Sim, pois você deseja substituir as concessões ativas.
   b. Usando a API `CreateGrantVersion`, ative a nova concessão especificando `ALL_GRANTS_PERMITTED_BY_ISSUER` para o `ActivationOverrideBehavior` com um `Status` de `Active`.

Console

Você pode usar o console do License Manager para ativar uma concessão. Ao ativar um subsídio proveniente do AWS Marketplace, você pode ter a opção de substituir os subsídios ativos:

- Como administrador de licenças, você precisar especificar se deseja substituir as concessões ativas ao ativar uma concessão.
- Como concedente, você pode, opcionalmente, especificar se deseja substituir as concessões ativas ao ativar uma concessão para outra conta em sua organização.
- Se o concedente não especificar se deseja substituir as concessões ativas, você, como beneficiário, precisará fazer essa seleção.

Como ativar uma licença (Console)

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças concedidas.

3. Escolha um ID de licença para abrir a página Visão geral da licença.
4. Escolha o nome de uma concessão para abrir a página Visão geral da concessão.
5. Se precisar, selecione uma opção de ativação para decidir se deseja substituir as concessões ativas:
   a. Não — Essa opção ativará a concessão sem substituir as já existentes para o destinatário (beneficiário).
   b. Sim — Essa opção desativará as concessões para o mesmo produto e ativará uma nova concessão para o destinatário definido (beneficiário):
      i. Um especificado Conta da AWS.
      ii. Contas de membros da UO da organização especificada.
      iii. Todas as contas de membros da organização.
6. (Opcional) Forneça um motivo para ativar a concessão.
7. Digite **`activate`** na caixa de entrada e escolha Ativar.

AWS CLI

Você pode usar o AWS CLI para trabalhar com suas licenças concedidas.

Para trabalhar com subsídios distribuídos usando AWS CLI:

- accept-grant
- create-grant-version
- list-received-grants
- list-received-grants-for-organization
- reject-grant

Status da licença para concessões no License Manager

As licenças têm dois status: o Status da licença, que mostra a disponibilidade e a capacidade de compartilhamento geral da licença, e o Status da concessão, que mostra a capacidade de usar a licença.

A tabela a seguir mostra os vários status de uma licença concedida:

Status	Description
DISPONÍVEL	A licença está disponível para uso e compartil hamento.
PENDENTE_DISPONÍVEL	A licença não está disponível para uso, pois ainda está sendo processada.
DESATIVADA	A licença não está disponível para uso porque foi desativada pelo emissor.
SUSPENSA	A licença não está disponível para uso, pois está suspensa.
EXPIRADA	A licença não está disponível para uso porque chegou ao fim do prazo.
PENDENTE_EXCLUÍDA	A licença não está disponível para uso, pois está sendo excluída.
EXCLUÍDA	A licença não está disponível para uso porque o contrato foi cancelado.

A tabela a seguir mostra os vários status de uma concessão:

Status	Description
PENDENTE_WORKFLOW	A concessão está em processo de distribuição.
PENDENTE_ACEITA	A concessão foi criada e o beneficiário ainda não a aceitou.
REJEITADA	A concessão foi rejeitada pelo destinatário.
ATIVA	A concessão foi aceita e ativada para uso pelo destinatário. O atributo licenciado pode ser usado.

Status	Description
FALHA_WORKFLOW	A distribuição da concessão falhou.
EXCLUÍDA	A concessão foi excluída pelo concedente.
PENDENTE_EXCLUÍDA	A concessão distribuída está em processo de ser excluída.
DESATIVADA	A concessão foi aceita pelo destinatário, mas não foi ativada para uso.
WORKFLOW_CONCLUÍDO	A concessão para uma organização foi distribuída ou retirada. Os detalhes da concessão mostram o status das subconcessões para cada conta na organização.

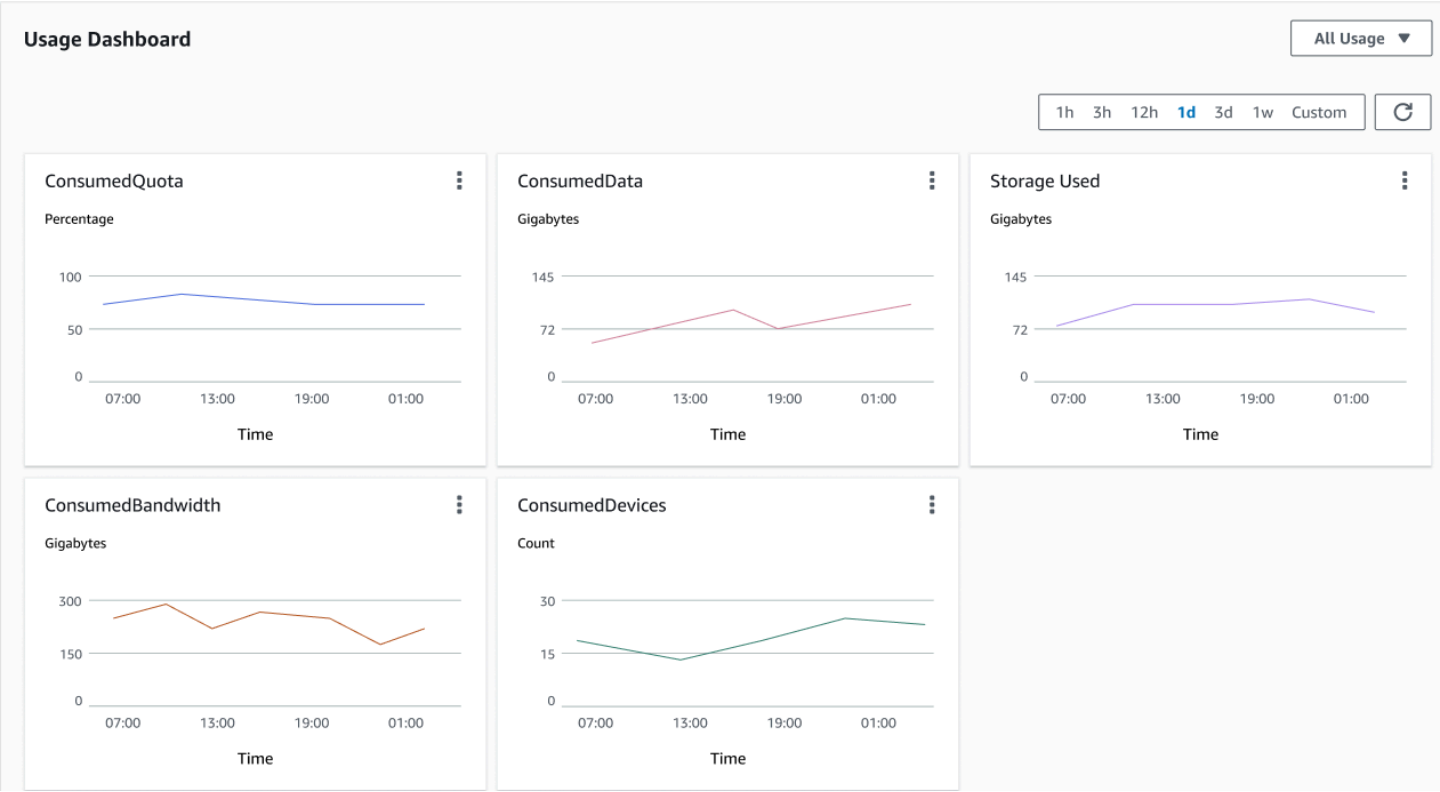
CloudWatch métricas para contas de compradores no License Manager

Quando uma concessão para uma licença emitida por um vendedor é configurada com a opção Permitir envio de registros de uso selecionada, o License Manager emite uma CloudWatch métrica para a conta do vendedor, a conta do comprador raiz e a conta na qual o uso está sendo registrado. As contas de compradores são Contas da AWS aquelas que compraram ou receberam uma licença emitida pelo vendedor. Para obter mais informações, consulte Conceder licenças a clientes.

Painel de uso

Quando um aplicativo vendedor ou fornecedor independente de software (ISV) registra o uso de uma licença para uma conta de comprador, a conta na qual o uso está sendo registrado e a conta raiz do comprador veem um CloudWatch widget com registros de uso na página do painel de uso no console do License Manager. Os compradores também podem ver métricas das contas para as quais distribuíram licenças no AWS Organizations. Os gráficos no Painel de uso estão disponíveis para todas as licenças que recebem registros de uso.

A imagem a seguir é um exemplo do painel de uso:



Análise de licenças

Os grupos de ativos de licença fornecem recursos abrangentes de painel e visualização que permitem que você tenha visibilidade do seu portfólio de licenciamento de software em todas as AWS regiões e contas da sua organização.

Conteúdo

Visualização do painel principal

O painel de grupos de ativos de licenças exibe seus 5 principais grupos de ativos de licença com base na contagem de instâncias com rastreamento de consumo em tempo real.

Seleção de intervalo de tempo

- Selecione entre: Últimos 1, 3, 6 ou 12 meses, ou intervalo de datas personalizado

- Use intervalos de datas flexíveis para identificar padrões sazonais e acompanhar tendências de crescimento

Visualizações interativas

- Passe o mouse sobre os gráficos para ver contagens detalhadas de instâncias
- Veja as tendências de uso em todos os tipos de licença:
  - Licenças autogerenciadas - BYOL de fornecedores de software
  - Licenças concedidas - Licenças fornecidas e AWS adquiridas pelo AWS Marketplace ou por terceiros

Visualização do grupo de ativos de licenças individuais

Selecione um grupo de ativos de licença no menu suspenso para ver informações detalhadas

Aba Resumo

Detalhes

- Número total de instâncias rastreadas dentro do grupo de ativos de licença
- Licenças concedidas rastreadas dentro do grupo de ativos de licença
- Licenças autogerenciadas rastreadas dentro do grupo de ativos de licenças

Próximas renovações

Lista de licenças que serão renovadas nos próximos 7, 30 ou 100 dias, monitoradas dentro do grupo de ativos de licenças

> **Note**
>
> Você deve configurar as datas de expiração da licença para ver as próximas renovações. Consulte Edite uma licença autogerenciada no License Manager.

Tendências de uso

As tendências de instância e licença exibem padrões de consumo de licenças para licenças autogerenciadas e concedidas durante o período selecionado rastreado dentro do grupo de ativos de licença

Para saber os detalhes sobre as métricas fornecidas pelo grupo de ativos de licença, consulte. Monitorando o License Manager com a Amazon CloudWatch

Crie um relatório de uso

AWS O License Manager fornece recursos abrangentes de geração de relatórios de uso para licenças autogerenciadas e grupos de ativos de licenças. Você pode gerar relatórios periódicos para licenças autogerenciadas ou relatórios sob demanda para grupos de ativos de licenças para monitorar o uso de licenças, a conformidade e o inventário de recursos em toda a sua organização.

Relatórios de licenças autogerenciados

Os relatórios de licença autogerenciados fornecem instantâneos periódicos do uso da sua licença. Você pode configurar vários relatórios de uso para rastrear diferentes tipos de licenças em seu ambiente com a publicação automática nos buckets do Amazon S3.

Relatório resumo de licenças autogerenciadas

Contém informações sobre o número de licenças consumidas e detalhes sobre configurações de licenças autogerenciadas, incluindo contagem de licenças, regras de licença e distribuição entre tipos de recursos.

Relatório de uso de atributos

Fornece detalhes sobre os recursos monitorados e seu consumo de licenças, listando cada recurso com informações de ID de licença, status e ID AWS da conta.

Para criar um relatório de uso de licenças autogerenciado

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Relatórios de uso (em Análise de licenças).
3. Escolha Criar relatório de uso e defina os parâmetros:
   a. Insira um nome e uma descrição opcional para o relatório.
   b. Selecione um tipo de licença autogerenciada na lista suspensa.

c. Escolha os tipos de relatório a serem gerados.

d. Escolha a frequência: uma vez a cada 24 horas, uma vez a cada 7 dias ou uma vez a cada 30 dias.

e. (Opcional) Adicione tags para rastrear o atributo relatório de uso.

4. Selecione Criar relatório de uso.

Para criar um relatório de licença autogerenciado usando a CLI

- Use o comando `create-license-manager-report-generator`:

```
aws license-manager create-license-manager-report-generator \
    --report-generator-name "Daily License Usage Report" \
    --type LicenseUsageReport \
    --report-context '{
      "licenseConfigurationArns": [
        "arn:aws:license-manager:region:account:license-configuration/lic-config-
id"
      ]
    }' \
    --report-frequency '{
      "value": 1,
      "period": "DAY"
    }' \
    --client-token unique-token
```

Relatórios de grupos de ativos de licença

Os relatórios de grupos de ativos de licença fornecem relatórios abrangentes e sob demanda para conformidade com licenças de software em várias AWS regiões e contas em sua organização. Esses relatórios oferecem um inventário detalhado de todos os recursos descobertos e mapeados para um grupo de ativos de licença.

Para criar um relatório de grupo de ativos de licença

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Relatórios de uso (em Análise de licenças).
3. Escolha Criar relatório de grupo de ativos de licença e defina os parâmetros:

a. Insira um nome e uma descrição opcional para seu relatório.

b. Selecione um grupo de ativos de licença na lista suspensa.

c. Escolha o intervalo de datas para listar todos os recursos dentro desse intervalo.

d. (Opcional) Adicione tags para rastrear o atributo relatório de uso.

4. Selecione Criar relatório de uso.

Para criar um relatório de grupo de ativos de licença usando a CLI

- Use o `create-license-manager-report-generator` comando para relatórios sob demanda com um intervalo de tempo específico:

```
aws license-manager create-license-manager-report-generator \
    --report-generator-name "License asset group Report" \
    --type LicenseAssetGroupReport \
    --report-context '{
      "licenseAssetGroupArns": [
        "arn:aws:license-manager:region:account:license-asset-group/group-id"
      ],
      "startTime": "2024-01-01T00:00:00Z",
      "endTime": "2024-01-31T23:59:59Z"
    }' \
    --client-token unique-token
```

> **Note**
>
> Os relatórios do grupo de ativos de licença são gerados sob demanda por um intervalo de tempo especificado e não oferecem suporte ao agendamento periódico. Omita o parâmetro `--report-frequency`.

Armazenamento de relatórios

Os relatórios de uso começam a ser publicados em 60 minutos. Se você ainda não tiver um bucket do Amazon S3 associado à sua conta, o License Manager criará um novo bucket do Amazon S3 quando você criar um relatório de uso. Os relatórios são armazenados com o seguinte padrão de URI do Amazon S3:

```
s3://aws-license-manager-service-*/Reports/usage-report-name/year/month/day/report-id.csv
```

Para obter mais informações sobre o comando CLI, consulte create-license-manager-report-generator ().AWS CLI

> **Note**
>
> AWS O License Manager não armazena seus relatórios. Os relatórios são publicados diretamente no seu bucket do Amazon S3. Depois de excluir um relatório de uso, os relatórios não são mais publicados no seu bucket do Amazon S3.

Pesquisa de inventário no License Manager

O License Manager permite descobrir aplicativos on-premises usando o Inventário do Systems Manager (SSM) e anexar regras de licenciamento a eles. Depois que as regras de licenciamento forem anexadas a esses servidores, você poderá rastreá-las junto com seus AWS servidores no painel do License Manager.

Para organizações que usam grupos de ativos de licenças, os resultados da pesquisa de inventário podem ser consolidados em várias AWS regiões e contas dentro de suas AWS organizações, fornecendo uma visão unificada dos recursos descobertos, independentemente de quais regiões ou contas eles residam.

O License Manager não pode, porém, validar regras de licenciamento para esses servidores no momento do lançamento ou encerramento. Para manter as informações sobre não AWS servidores atualizadas, você deve atualizar periodicamente as informações do inventário usando a seção Pesquisa de inventário do console do License Manager.

O Systems Manager armazena dados nos dados de Inventário por 30 dias. Durante esse período, o License Manager conta uma instância gerenciada como ativa até mesmo se ela não for compatível com ping. Assim que os dados de inventário forem eliminados do Systems Manager, o License Manager marcará a instância como inativa e atualizará os dados de inventário local. Para manter as contagens de instâncias gerenciadas precisas, recomendamos cancelar o registro das instâncias manualmente no Systems Manager, para que o License Manager possa executar operações de limpeza.

A consulta do inventário do Systems Manager requer uma sincronização de dados de recursos para armazenar o inventário em um bucket do Amazon S3, e o Amazon Athena para agregar dados de inventário de contas organizacionais AWS Glue e fornecer uma experiência de consulta rápida. Para obter mais informações, consulte Usando funções vinculadas a serviços para o License Manager.

O rastreamento do inventário de recursos também é útil se sua organização não impede que AWS os usuários criem AMI-derived instâncias ou instalem software adicional em instâncias em execução. O License Manager fornece um mecanismo para descobrir facilmente essas instâncias e aplicativos usando a pesquisa de inventário. Você pode anexar regras a esses atributos descobertos e rastreá-los e validá-los como instâncias criadas de AMIs gerenciadas.

Conteúdo

Trabalhe com a pesquisa de inventário no License Manager

O License Manager usa o Inventário do Systems Manager para descobrir o uso de software on-premises. Depois que você associa uma licença autogerenciada a servidores on-premises, o License Manager coleta periodicamente o inventário de software, atualiza as informações de licenciamento e atualiza seus painéis para criar relatórios sobre o uso.

Tarefas

Configurar para pesquisa de inventário

Preencha os seguintes requisitos antes de usar a pesquisa de inventário de atributos:

- Permita a descoberta de inventário entre contas integrando o License Manager à sua AWS Organizations conta. Para obter mais informações, consulte Configurações no License Manager.

- Crie licenças autogerenciadas para gerenciar os servidores e aplicativos. Por exemplo, crie uma licença autogerenciada que reflita os termos do seu contrato de licenciamento com a Microsoft para o SQL Server Enterprise.

Use a pesquisa de inventário

Conclua as etapas a seguir para pesquisar no seu inventário de atributos. Você pode pesquisar aplicativos por nome (por exemplo, nomes que começam com “SQL Server”) e pelo tipo de licença incluída (por exemplo, uma licença que não seja para “SQL Server Web”).

Pesquise seu inventário de recursos

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Pesquisa de inventário.
3. (Opcional) Você pode especificar as opções de filtro para simplificar os resultados da pesquisa da seguinte maneira.

   Recursos do Amazon EC2

Nome do filtro	Description	Operadores lógicos	Valores com suporte
Resource ID (ID do recurso)	O ID do recurso.	`Equals`, `Not equals`	
ID da conta	O ID da AWS conta que possui o recurso.	`Equals`, `Not equals`	
nome-da-plataforma	A plataforma do sistema operacional para o recurso.	`Equals`, `Not equals`, `Begins with`, `Contains`	
Nome da aplicação	O nome da aplicação .	`Equals`, `Begins with`	
Nome incluído na licença	O tipo de licença incluída.		•

Nome do filtro	Description	Operadores lógicos	Valores com suporte
		`Equals`, `Not equals`	• `SQL Server Enterprise` • `SQL Server Standard` • `SQL Server Web` • `Windows Server Datacenter`
Tag	Uma chave de tag de metadados e um valor opcional atribuído ao recurso. Observe que o operador `Not equals` lógico só estará disponível se a descoberta entre contas estiver ativada.	`Equals`, `Not equals`	

Recursos do Amazon RDS

Nome do filtro	Description	Operadores lógicos	Valores com suporte
Edição do mecanismo	A edição do mecanismo de banco de dados.	`Equals`	• `oracle-ee` • `oracle-se` • `oracle-se1` • `oracle-se2` • `db2-se` • `db2-ae` • `sqlserver-ee` • `sqlserver-se`

Nome do filtro	Description	Operadores lógicos	Valores com suporte
Pacote de licenças (somente Oracle)	O pacote de gerenciamento associado a uma licença do Amazon RDS for Oracle.	`Equals`	• `Spatial and Graph` • `Active Data Guard` • `Label Security` • `Oracle On-Line Analytical Processing (OLAP)` • `Diagnosti c Pack and Tuning Pack`

Para obter mais informações sobre as licenças de produtos de banco de dados do Amazon RDS, consulte as opções de licenciamento do RDS para Oracle, as opções de licenciamento do RDS para DB2 ou as opções de licenciamento do RDS para SQL Server no Guia do usuário do Amazon RDS.

Adicione regras de descoberta automatizada a uma licença autogerenciada

Depois de adicionar informações do produto à sua licença autogerenciada, o License Manager pode rastrear o uso da licença para as instâncias que têm esses produtos instalados. Para obter mais informações, consulte Descoberta automatizada do inventário no License Manager.

Para adicionar regras de descoberta automatizada a uma licença autogerenciada

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Abra a página de Pesquisa de inventário.

3. Selecione o atributo e escolha Adicionar regras de descoberta automatizada.
4. Para Self-managed licença, selecione uma licença autogerenciada.
5. Especifique os produtos que você quer descobrir e rastrear.
6. (Opcional) Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.
7. (Opcional) Para excluir recursos da descoberta automática, selecione Adicionar regra de exclusão.

   > **Note**
   >
   > As regras de exclusão não se aplicam aos produtos Amazon RDS (como RDS for Oracle, RDS for Db2 e RDS for SQL Server).

   a. Escolha uma Propriedade para filtrar. Atualmente, há suporte para ID da conta e Tag.
   b. Insira informações para identificar essa propriedade. Para um ID da conta, especifique o ID da AWS conta de 12 dígitos como o valor. Para Tags, insira um key/value par.
   c. Repita a etapa 7 para adicionar regras adicionais.
8. Escolha Adicionar.

Associe uma licença autogerenciada à pesquisa de inventário

Depois de identificar os atributos não gerenciados que você precisa gerenciar, é possível associá-los manualmente a uma licença autogerenciada, em vez de usar a descoberta automatizada.

Para associar uma licença autogerenciada a um atributo

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Abra a página de Pesquisa de inventário.
3. Selecione o atributo e escolha Associar licença autogerenciada.
4. Para Nome da licença autogerenciada, selecione uma licença autogerenciada.
5. (Opcional) Selecione Compartilhar licença autogerenciada com todas as contas-membro.
6. Selecione Associar .

Desassociar uma licença autogerenciada e um recurso

Se os termos de licenciamento de seus fornecedores de software mudarem, é possível desassociar atributos que foram associados manualmente e excluir a licença autogerenciada.

Para desassociar uma licença autogerenciada de um atributo

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Licença autogerenciada.
3. Selecione o nome da licença autogerenciada.
4. Escolha atributos.
5. Selecione os atributos que você deseja desassociar da licença autogerenciada e depois clique em Desassociar atributo.

Descoberta automatizada do inventário no License Manager

O License Manager usa o Inventário do Systems Manager para descobrir o uso de software nas instâncias do Amazon EC2 o em instâncias on-premises. Você pode adicionar informações do produto à sua licença autogerenciada, e o License Manager rastreará as instâncias que têm esses produtos instalados. Além disso, você pode especificar regras de exclusão com base no seu contrato de licenciamento para decidir quais instâncias excluir. Você pode excluir instâncias pertencentes a IDs de contas da AWS ou instâncias associadas a tags de atributos. Assim, elas não serão consideradas para a descoberta automatizada.

A descoberta automatizada pode ser adicionada a um novo conjunto de licenças, a uma licença autogerenciada existente ou a atributos do seu inventário. As regras para descoberta automatizada podem ser editadas a qualquer momento por meio da CLI usando o comando UpdateLicenseConfigurationAPI. Para editar regras no console, exclua a licença autogerenciada existente e crie uma nova.

Para usar a descoberta automatizada, adicione informações do produto à sua licença autogerenciada. Você pode fazer isso ao criar a licença autogerenciada usando a Pesquisa de inventário.

Você não pode desassociar manualmente as instâncias rastreadas pela descoberta automatizada. Por padrão, a descoberta automatizada não dissocia as instâncias rastreadas após a desinstalação do software. Você pode configurar a descoberta automatizada para que ela interrompa o rastreamento de instâncias quando o software for desinstalado.

Depois de fazer isso, você pode acompanhar o uso de licenças pelo painel do License Manager.

Pré-requisitos

- Habilite a pesquisa de inventário entre contas integrando o License Manager à sua AWS Organizations conta. Para obter mais informações, consulte Configurações no License Manager.

> **Note**
>
> Contas individuais podem configurar a descoberta automatizada, mas não podem adicionar regras de exclusão.

- Instale o inventário do Systems Manager em suas instâncias.

Para configurar a descoberta automatizada ao criar uma licença autogerenciada

Você pode configurar regras automatizadas de descoberta e regras de exclusão ao criar uma licença autogerenciada. Para obter mais informações, consulte Crie uma licença autogerenciada no License Manager.

Para adicionar regras de descoberta automatizada a uma licença autogerenciada

Use o processo abaixo para adicionar regras de descoberta automatizada às licenças autogerenciadas existentes usando o console. Você também pode fazer isso no painel Pesquisa de inventário, selecionando um ID de atributo e clicando em Adicionar regras de descoberta automatizada.

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, escolha Self-managed licenças.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Na guia Regras de descoberta automatizada, escolha Adicionar regras de descoberta automatizada.
5. Especifique os produtos que você quer descobrir e rastrear.

> **Note**
>
> As seguintes limitações se aplicam aos produtos de banco de dados Amazon RDS (como Amazon RDS for Oracle, Amazon RDS for Db2 e Amazon RDS for SQL Server):

- Há suporte para no máximo uma regra especificando um produto de banco de dados Amazon RDS.
- Somente uma configuração de licença é permitida para cada produto de banco de dados do Amazon RDS.

6. (Opcional) Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.
7. (Opcional) Para definir atributos a serem excluídos da descoberta automatizada, selecione Adicionar regra de exclusão.

> **Note**
>
> - As regras de exclusão não se aplicam aos produtos de banco de dados do RDS (como Amazon RDS para Oracle, Amazon RDS para Db2 e Amazon RDS for SQL Server).
> - As regras de exclusão só estão disponíveis se o Descoberta de atributos entre contas estiver ativado.

   a. Escolha uma Propriedade para filtrar. Atualmente, há suporte para ID da conta e Tag.
   b. Insira informações para identificar essa propriedade. Para um ID de conta, especifique o ID da AWS conta de 12 dígitos como o valor. Para Tags, insira um key/value par.
   c. Repita a etapa 7 para adicionar regras adicionais.
8. Ao terminar, escolha Adicionar para aplicar sua regra de descoberta automatizada.

Conversões de tipo de licença no License Manager

Com o License Manager, você pode alterar o tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) conforme as necessidades de sua empresa mudarem. É possível fazer isso sem reimplantar suas workloads existentes.

Você pode otimizar seu inventário de licenças para os seguintes cenários usando a conversão:

Migrar workloads on-premises para o Amazon EC2

Durante a migração, você pode implantar sua carga de trabalho no Amazon Elastic Compute Cloud (Amazon AWS EC2) e usar as licenças fornecidas. Quando a migração estiver concluída, use a Conversão de tipo de licença do License Manager para alterar o tipo de licença de suas instâncias. Você pode mudar para BYOL para poder usar as licenças que foram liberadas durante a migração.

Continue executando workloads com contratos de licença expirados

Você pode usar a conversão do tipo de licença do License Manager para mudar de BYOL para licenças AWS fornecidas. Essa opção permite que você continue executando suas cargas de trabalho com licenças de software totalmente compatíveis, fornecidas por um modelo flexível de licenciamento AWS go. pay-as-you Você pode fazer isso caso seu contrato de licença com o fornecedor do software do sistema operacional (A Microsoft ou a Canonical, por exemplo) estiver prestes a expirar e você não planejar renová-lo.

Otimize custos

Para cargas de trabalho pequenas ou irregulares, as instâncias com licenças AWS fornecidas (licença incluída) podem ser mais econômicas. Quando você opta por usar o BYOL, essas opções podem exigir um compromisso de longo prazo. Nesse caso, você pode usar a Para obter mais informações do License Manager para mudar suas instâncias para licença incluída, otimizando os custos relacionados ao licenciamento. Se suas instâncias foram iniciadas a partir da sua própria imagem de máquina virtual (VM), você pode voltar para o BYOL. Isso pode ser feito quando a workload for mais estável ou previsível.

Manutenção estendida

Se o seu sistema operacional Ubuntu chegou ao fim do suporte padrão, você pode adicionar uma assinatura paga do Ubuntu Pro. Adicionar uma assinatura ao Ubuntu on Pro fornece atualizações de segurança por um longo período de tempo. Para obter mais informações, consulte Ubuntu Pro na documentação da Canonical.

Tópicos

- Solução de problemas de conversão de tipo de licença no License Manager

Tipos de licença elegíveis para conversão de tipo de licença no License Manager

Você pode usar a conversão de tipo de licença do License Manager com versões compatíveis e combinações de licenças do Windows Server e do Microsoft SQL Server. Você também pode usar a conversão de tipo de licença com assinaturas do Ubuntu Linux.

Sumário

Tipos de licença elegíveis para Windows e SQL Server no License Manager

> **Important**
>
> Instâncias originalmente lançadas a partir de uma imagem de máquina da Amazon (AMI) fornecida pela Amazon não estão qualificadas para conversão para BYOL.

O Windows e o SQL Server devem atender a determinados requisitos para se qualificarem para a conversão de tipo de licença.

Tópicos

- Compatibilidade de mídia
- Caminhos de conversão

Edições do SQL Server

O License Manager oferece suporte às seguintes edições do SQL Server:

- SQL Server Standard Edition
- SQL Server Enterprise Edition
- SQL Server Web Edition

Versão do SQL Server

O License Manager oferece suporte às seguintes versões do SQL Server:

- SQL Server 2005
- SQL Server 2008
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

Valores da operação de uso

Uma conversão de tipo de licença altera o valor da operação de uso associado à sua instância. Os valores da operação de uso para cada sistema operacional compatível são fornecidos na tabela a seguir. Para obter mais informações, consulte os campos de informações de faturamento da AMI.

Detalhes do sistema operacional	Operação de uso
Windows Server como BYOL	RunInstances0800

Detalhes do sistema operacional	Operação de uso
Windows Server como BYOL SQL Server (qualquer edição) como BYOL	RunInstances0800
Windows Server como licença incluída	RunInstances:002
Windows Server como licença incluída SQL Server (qualquer edição) como BYOL	RunInstances:002
Windows Server como licença incluída SQL Server Web como licença incluída	RunInstances0:02
Windows Server como licença incluída SQL Server Standard como licença incluída	RunInstances0:006
Windows Server como licença incluída SQL Server Enterprise como licença incluída	RunInstances0:012

Compatibilidade de mídia

A tabela a seguir confirma quais mídias podem ser usadas em quais modelos de licenciamento de instância.

Fonte	Destino	
	BYOL	Licença incluída
	Não	Sim

Fonte	Destino	
AWS imagem fornecida do Windows Server		
AWS imagem fornecida do SQL Server	Não	Sim
Sua mídia do Windows Server[1]	Sim	Sim
Sua mídia do SQL Server[2]	Sim	Sim

[1] Indica que a instância foi originalmente iniciada a partir de sua própria máquina virtual (VM) importada. Você pode importar sua VM usando um serviço como o VM Import/Export ou o AWS Transform MGN.

[2] Indica que você adquiriu sua própria mídia de instalação do SQL Server (.iso, .exe).

Caminhos de conversão

A tabela a seguir confirma se o modelo de licença de origem pode ser convertido para outro modelo, entre BYOL e licença incluída. Para obter mais informações, consulte Converter um tipo de licença no License Manager.

> **Important**
>
> - O Windows Server como BYOL com o SQL Server como licença incluída é uma configuração incompatível.
> - As conversões especificadas como “Não necessárias” não alterarão o valor da operação de uso.

Fonte	Destino

Fonte	Destino					
	Windows Server como BYOL	Windows Server como licença incluída	Windows Server como BYOL SQL Server como BYOL	Windows Server como licença incluída SQL Server como BYOL	Windows Server como BYOL SQL Server como licença incluída	Windows Server como licença incluída SQL Server como licença incluída
Windows Server como BYOL (sua mídia)	Não é necessário	Sim	Não é necessário	Sim[1]	Sem suporte	Sim[1]
Windows Server como licença incluída (sua mídia)	Sim[2]	Não é necessário	Sim [1, 2]	Não é necessário [3]	Sem suporte	Sim[1]
Windows Server como licença incluída (imagem AWS fornecida)	Não ✗	Não é necessário	Não ✗	Não é necessário [3]	Sem suporte	Sim[3]

Fonte	Destino					
Windows Server como BYOL (sua mídia)	Não é necessário [4]	Sim	Não é necessário	Sim	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						
Windows Server como licença incluída (sua mídia)	Sim [2]	Não é necessário [4]	Sim [2]	Não é necessário	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						

Fonte	Destino					
Windows Server como licença incluída (imagem AWS fornecida)	Não ✗	Não é necessário [4]	Não ✗	Não é necessário	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						
Windows Server como BYOL (sua mídia)	Sem suporte	Sem suporte	Sem suporte	Sem suporte	Sem suporte	Sem suporte
SQL Server como licença incluída						

Fonte	Destino					
Windows Server como licença incluída (imagem AWS fornecida ou sua mídia)	Não ✗	Não ✗	Não ✗	Não ✗	Sem suporte	Não é necessário
SQL Server como licença incluída (imagem AWS fornecida)	Sim [2, 5, 6]	Sim [5]	Sim [2]	Sim	Sem suporte	Não é necessário
Windows Server como licença incluída (sua mídia)						
SQL Server como licença incluída (sua mídia)						

Fonte	Destino					
Windows Server como licença incluída (imagem AWS fornecida)	Não ✗	Sim[5]	Não ✗	Sim	Sem suporte	Não é necessário
SQL Server como licença incluída (sua mídia)						

✗ Você deve implantar uma nova instância com uma configuração alternativa, pois a conversão para os tipos de licença de destino não são compatíveis. Para obter mais informações, consulte Compatibilidade de mídia.

Para outros cenários de conversão, talvez seja necessário seguir as etapas a seguir:

[1] Primeiro instale o SQL Server antes de converter para “BYOL para SQL Server”.

[2] Primeiro modifique a configuração do Windows para usar seu próprio servidor KMS para ativação da licença. Para obter mais informações, consulte Convert Windows Server from license included to BYOL.

[3] Primeiro instale o SQL Server ao converter de uma origem sem o SQL Server para um destino com o SQL Server (independentemente do tipo de licença).

[4] Primeiro desinstale o SQL Server ao converter de uma origem com o SQL Server para um destino sem o SQL Server (independentemente do tipo de licença).

[5] Primeiro desinstale o SQL Server antes de converter para o SQL Server com licença incluída.

[6] Primeiro execute as etapas para [2] e [5]. Depois que essas etapas forem concluídas, converta o tipo de licença para Windows Server como licença incluída e, em seguida, converta o tipo de licença mais uma vez para Windows Server como BYOL.

Tipos de assinatura elegíveis para Linux no License Manager

A conversão de tipo de licença está disponível para versões compatíveis do Ubuntu. As versões compatíveis incluem atualizações como o Ubuntu 18.04.1 LTS. Quando você converte uma assinatura para o Ubuntu Pro, as atualizações de segurança são fornecidas por mais cinco anos. Para obter mais informações, consulte Ubuntu Pro na documentação da Canonical.

Você pode usar a conversão de tipo de licença para versões de suporte de longo prazo (LTS) do Ubuntu, RHEL e RHEL para SAP. Você pode alternar as assinaturas entre as opções AWS fornecidas e fornecidas pela Red Hat em. AWS Marketplace

Considerações sobre a conversão de tipo de licença

Algumas das considerações às quais a conversão de tipo de licença está sujeita estão listadas a seguir. Esta é uma lista incompleta e sujeita a alterações.

RHEL e RHEL para conversão de SAP

- Se você estiver convertendo para assinaturas vendidas pela Red Hat como uma listagem de AMI, AWS Marketplace você deve primeiro assinar a lista de AMI do Marketplace antes de iniciar a conversão da licença.
- Para fazer as transições para a listagem AWS Marketplace SaaS do Red Hat Subscriptions, você precisa comprar assinaturas da Red Hat antes da conversão.
- Se você tiver um contrato anual da Red Hat, AWS Marketplace você não receberá reembolso por meses não utilizados ao converter para outro tipo de assinatura.
- Para converter de RHEL para SAP vendido pela Red Hat em AWS Marketplace RHEL para SAP vendido por AWS , AWS Marketplace envie uma solicitação para. Suporte Para obter mais informações, consulte Criar um caso de suporte.

Conversão do Ubuntu

- A instância deve estar executando o Ubuntu LTS para converter o tipo de licença para Ubuntu Pro.
- Você não pode usar a conversão de tipo de licença para uma assinatura do Ubuntu Pro. Para remover uma assinatura do Ubuntu Pro, consulte Como remover uma assinatura do Ubuntu Pro.

- O Ubuntu Pro não está disponível como uma instância reservada. Para obter economias significativas em comparação com os preços de instâncias sob demanda, recomendamos usar o Ubuntu Pro com Savings Plans. Para obter mais informações, consulte Instâncias reservadas no Guia do usuário do Amazon EC2 e What are Savings Plans? no Guia do usuário do Savings Plans.
- Para converter do Ubuntu Pro para o Ubuntu LTS, envie uma solicitação para Suporte. Para obter mais informações, consulte Criar um caso de suporte.

Pré-requisitos de conversão para os tipos de licença do License Manager

Para converter tipos de licença com o License Manager, existem pré-requisitos gerais e específicos de cada sistema operacional.

Tópicos

Geral

Você deve atender aos seguintes pré-requisitos gerais antes de realizar uma conversão de tipo de licença:

- Você Conta da AWS deve estar integrado ao License Manager. Consulte Comece a usar o License Manager.
- A instância de destino deve ser executada em AWS. Não há suporte para instâncias locais.
- A instância de destino deve estar no estado interrompido antes de você converter o tipo de licença. Para obter mais informações, consulte Encerrar e iniciar sua instância no Guia do Usuário do Amazon EC2.
- Se a proteção contra interrupção estiver ativada na instância de destino, o processo de conversão falhará. Para obter mais informações, consulte Solução de problemas de conversão de tipo de licença no License Manager.
- A instância de destino deve ser configurada com o AWS Systems Manager Inventory. Para obter mais informações, consulte Configuração do Systems Manager para instâncias do EC2 e Inventário do AWS Systems Manager no Guia do usuário do AWS Systems Manager .
- Sua usuário ou perfil precisa incluir as seguintes permissões:

- `ssm:GetInventory`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `license-manager:CreateLicenseConversionTaskForResource`
- `license-manager:GetLicenseConversionTask`
- `license-manager:ListLicenseConversionTasks`
- `license-manager:GetLicenseConfiguration`
- `license-manager:ListUsageForLicenseConfiguration`
- `license-manager:ListLicenseSpecificationsForResource`
- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`

Para obter mais informações sobre o Systems Manager Inventory, consulte AWS Systems Manager Inventory.

Windows

As instâncias do Windows devem atender aos seguintes pré-requisitos:

- Instâncias originalmente lançadas a partir de uma imagem de máquina da Amazon (AMI) fornecida pela Amazon não estão qualificadas para conversão para BYOL. A instância original do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM). Para obter mais informações sobre a conversão de uma VM para o Amazon EC2, consulte VM Import/Export.
- Para alterar sua licença do SQL Server para BYOL, o SQL Server deve ter sido instalado usando sua própria mídia.

Linux

As instâncias do Linux devem atender aos seguintes pré-requisitos:

RHEL

- Ao converter assinaturas AWS fornecidas em assinaturas vendidas pela Red Hat como uma listagem de AMI na AWS Marketplace, você deve primeiro assinar a lista de AMI do Marketplace da Red Hat antes de iniciar a conversão da licença.
- Para fazer a transição das assinaturas AWS fornecidas para a listagem SaaS do Red Hat Subscriptions, AWS Marketplace você precisará comprar assinaturas da Red Hat antes da conversão.

RHEL for SAP

- Para conversões do RHEL para SAP e do Update Services, as instâncias devem ser iniciadas AWS Marketplace com uma operação de RunInstance uso: 0010 e um código de produto anexado. AWS Marketplace
- Ao converter assinaturas AWS fornecidas em assinaturas vendidas pela Red Hat como uma listagem de AMI na AWS Marketplace, você deve primeiro assinar a lista de AMI do Marketplace da Red Hat antes de iniciar a conversão da licença.
- Para fazer a transição das assinaturas AWS fornecidas para a listagem SaaS do Red Hat Subscriptions, AWS Marketplace você precisará comprar assinaturas da Red Hat antes da conversão.

Ubuntu

- As instâncias precisam estar executando o Ubuntu LTS.
- O Ubuntu Pro Client precisa estar instalado no seu sistema operacional Ubuntu.
  - Para confirmar se o Ubunto Pro Client está instalado, execute o seguinte comando:

    ```
    pro --version
    ```

  - Se o comando não for encontrado ou se a versão precisar ser atualizada, execute o seguinte comando para instalar o Ubuntu Pro Client:

    ```
    apt-get update && apt-get dist-upgrade
    ```

- As instâncias devem ser capazes de alcançar vários endpoints para ativar a assinatura do Ubuntu Pro e receber atualizações. Você deve permitir que o tráfego que sai da sua instância pela porta TCP 443 alcance os seguintes endpoints:
  - contracts.canonical.com: usado para ativação do Ubuntu Pro.
  - esm.ubuntu.com: usado para acesso ao repositório APT para a maioria dos serviços.
  - api.snapcraft.io: usado para instalar e executar snaps.
  - dashboard.snapcraft.io: usado para instalar e executar snaps.
  - login.ubuntu.com: usado para instalar e executar snaps.
  - cloudfront.cdn.snapcraftcontent.com — Usado para baixar de redes de desenvolvimento de conteúdo (). CDNs
  - livepatch.canonical.com: usado para baixar correções do servidor Livepatch.

  Para obter mais informações, consulte Ubuntu Pro Client network requirements na documentação do Ubuntu Pro Client e Network requirements na documentação do Canonical Snapcraft.

Converter um tipo de licença no License Manager

Você pode converter licenças do Windows, licenças do Microsoft SQL Server e assinaturas do Ubuntu Linux usando o console do License Manager ou o AWS CLI. Talvez seja necessário concluir etapas adicionais para converter a licença ou a assinatura no sistema operacional da instância.

Você pode converter tipos de licença usando o console do License Manager ou o AWS CLI. Quando você cria uma conversão de tipo de licença, o License Manager valida os produtos de faturamento na sua instância. Se essas validações preliminares forem bem-sucedidas, o License Manager cria uma conversão de tipo de licença. Você pode verificar o status de uma conversão de tipo de licença usando os `get-license-conversion-task` AWS CLI comandos `list-license-conversion-tasks` e.

O License Manager pode atualizar os atributos associados às suas licenças autogerenciadas como parte de uma conversão de tipo de licença. Especificamente, para qualquer licença autogerenciada com regras de descoberta automatizada do tipo `License Included`, o License Manager desassocia o atributo da licença durante conversão, se a regra `license included` excluir explicitamente o atributo.

Por exemplo, se sua licença autogerenciada contiver duas regras de descoberta automatizada e cada regra excluir o Windows Server com licença incluída, uma conversão de BYOL para Windows

Server com licença incluída resultará na dissociação entre a instância e a licença autogerenciada. No entanto, se apenas uma das duas regras contiver uma regra `License Included`, a instância não será dissociada.

Não inicie nem interrompa sua instância enquanto a conversão de tipo de licença estiver em andamento. Quando a conversão é bem-sucedida, seu status muda de `IN_PROGRESS` para `SUCCEEDED`. Se o License Manager encontrar problemas durante o fluxo de trabalho, ele atualiza o status da conversão para `FAILED` e a mensagem de status vira uma mensagem de erro.

> **Note**
>
> As informações do produto de faturamento na AMI usadas para iniciar uma instância não mudam quando você converte o tipo de licença. Para recuperar informações de faturamento precisas, use a API `DescribeInstances` do Amazon EC2. Além disso, se você tiver fluxos de trabalho existentes que pesquisam informações de cobrança AMIs, atualize esses fluxos de trabalho para usá-los. `DescribeInstances`

Sumário

        - Conversão de Red Hat Enterprise Linux (RHEL) AWS para Red Hat License-Included (LI)
    - Conversão de assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) para Red Hat License-Included (LI)
    - Outros requisitos
    - Como converter para Ubuntu Pro
- Como remover uma assinatura do Ubuntu Pro

Converter um tipo de licença para Windows e SQL Server no License Manager

Você pode usar o License Manager Console ou o AWS CLI para converter o tipo de licença das instâncias elegíveis do Windows e do SQL Server.

Tópicos

- Limites da conversão de tipo de licença
- Como converter um tipo de licença usando o console do License Manager
- Converta um tipo de licença usando o AWS CLI

Limites da conversão de tipo de licença

> **Important**
>
> O uso de software da Microsoft está sujeito aos termos de licenciamento da Microsoft. Você é responsável por cumprir os termos de licenciamento da Microsoft. Esta documentação é fornecida por conveniência e você não pode confiar em sua descrição. Esta documentação não constitui aconselhamento jurídico. Se tiver dúvidas sobre seus direitos de licenciamento relacionados aos softwares da Microsoft, consulte sua equipe jurídica, a Microsoft ou seu revendedor da Microsoft.

O License Manager restringe os tipos de conversões de licença que você pode criar de acordo com o Contrato de Licenciamento do Provedor de Serviços da Microsoft (SPLA). Algumas das restrições às quais a conversão de tipo de licença está sujeita estão listadas a seguir. Esta é uma lista incompleta e sujeita a alterações.

- A instância do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM).
- O SQL Server com licença incluída não pode ser executado em um host dedicado.
- Uma instância do SQL Server com licença incluída deve ter pelo menos 4 v. CPUs

Como converter um tipo de licença usando o console do License Manager

Você pode usar o console do License Manager para converter um tipo de licença.

> **Note**
>
> Somente as instâncias em estado interrompido e associadas pelo Inventário do AWS Systems Manager são exibidas.

Para iniciar uma conversão de tipo de licença no console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, escolha Conversão de tipo de licença e, em seguida, escolha Criar conversão de tipo de licença.
3. Em Sistema operacional de origem, escolha a plataforma da instância que você deseja converter:
   - RHEL
   - RHEL para SAP
   - Ubuntu LTS
   - BYOL do Windows
   - Windows com licença incluída
4. (Opcional) Filtre as instâncias disponíveis especificando um valor para o ID da instância ou para ovalor da operação de uso.
5. Selecione as instâncias cujas licenças você deseja converter e escolha Avançar.
6. Insira o valor da operação de uso para o tipo de licença, selecione a licença para a qual você está convertendo e escolha Avançar.
7. Verifique se está satisfeito com a configuração da conversão de tipo de licença e escolha Iniciar conversão.

Você pode ver o status da conversão de tipo de licença no painel correspondente. A coluna “Status da conversão” exibe o status da conversão, como Em andamento, Concluída ou Com falha.

> **Important**
>
> Se você converter o Windows Server de licença incluída para BYOL, ative o Windows de acordo com seu contrato de licença da Microsoft. Consulte Convert Windows Server from license included to BYOL para obter mais informações.

Converta um tipo de licença usando o AWS CLI

Para iniciar uma conversão de tipo de licença no AWS CLI:

Determine o tipo de licença da instância

1. Verifique se você instalou e configurou o AWS CLI. Para obter mais informações, consulte Instalar, atualizar e desinstalar o AWS CLI e Configuração do AWS CLI.

   > **Important**
   >
   > Talvez seja necessário atualizar o AWS CLI para executar determinados comandos e receber todas as saídas necessárias nas etapas a seguir.

2. Verifique se você tem permissões para executar o `create-license-conversion-task-for-resource` AWS CLI comando. Para obter ajuda, consulte Criar políticas do IAM para o License Manager.
3. Para determinar o tipo de licença atualmente associado à sua instância, execute o AWS CLI comando a seguir. Substitua o ID da instância pelo ID da instância cujo tipo de licença você quer determinar.

   ```
   aws ec2 describe-instances --instance-ids <instance-id> --query
    "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
    PlatformDetails, ProductCode: ProductCode, UsageOperation: UsageOperation,
    UsageOperationUpdateTime: UsageOperationUpdateTime}"
   ```

4. O seguinte é um exemplo de resposta ao comando `describe-instances`. Observe que o valor `UsageOperation` é o código de informações de faturamento associado à licença.

`UsageOperationUpdateTime` é a hora em que o código de faturamento foi atualizado. Para obter mais informações, consulte DescribeInstances na Referência de API do Amazon EC2.

```
"InstanceId": "i-0123456789abcdef",
"Platform details": "Windows with SQL Server Enterprise",
"UsageOperation": "RunInstances:0800",
"UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
```

> **Note**
>
> A operação de uso do Windows Server com o SQL Server Enterprise BYOL é igual à operação de uso do Windows BYOL, já que elas são cobradas de forma idêntica.

Como converter o Windows Server de licença incluída para BYOL

Quando você converte o Windows Server de licença incluída para BYOL, o License Manager não ativa automaticamente o Windows. Você deve alternar o servidor KMS da sua instância do servidor AWS KMS para o seu próprio servidor KMS.

> **Important**
>
> Para converter de licença incluída para BYOL, a instância original do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM). Para obter mais informações sobre a conversão de uma VM para o Amazon EC2, consulte VM Import/Export. Instâncias originalmente lançadas a partir de uma Imagem de Máquina da Amazon (AMI) não estão qualificadas para conversão para BYOL.

Verifique o contrato de licença da Microsoft para determinar quais métodos você pode usar para ativar o Microsoft Windows Server. Por exemplo, se você estiver usando um servidor KMS, obtenha o endereço do servidor KMS da configuração BYOL original da instância.

1. Para converter o tipo de licença da sua instância, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
aws license-manager create-license-conversion-task-for-resource \
 --resource-arn <instance_arn> \
```

```
 --source-license-context UsageOperation=RunInstances:0002 \
 --destination-license-context UsageOperation=RunInstances:0800
```

2. Para ativar o Windows depois de converter sua licença, aponte o servidor KMS do Windows Server do seu sistema operacional para seus próprios servidores KMS. Faça login na instância do Windows e execute o seguinte comando:

```
slmgr.vbs /skms <your-kms-address>
```

Como converter o Windows Server de BYOL para licença incluída

Quando você converte o Windows Server de BYOL para a licença incluída, o License Manager muda automaticamente o servidor KMS da sua instância para o servidor AWS KMS.

Para converter o tipo de licença da sua instância de BYOL para licença incluída, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
aws license-manager create-license-conversion-task-for-resource \
 --resource-arn <instance_arn> \
 --source-license-context UsageOperation=RunInstances:0800 \
 --destination-license-context UsageOperation=RunInstances:0002
```

Converta o Windows Server e o SQL Server de BYOL para a licença incluída

É possível alterar vários produtos ao mesmo tempo. Por exemplo, é possível converter o Windows Server e SQL Server em uma única conversão.

Para converter o tipo de licença da sua instância do Windows Server de BYOL para licença incluída, e o SQL Server Standard de BYOL para licença incluída, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
aws license-manager create-license-conversion-task-for-resource \
 --resource-arn <instance_arn> \
 --source-license-context UsageOperation=RunInstances:0800 \
 --destination-license-context UsageOperation=RunInstances:0006
```

Converter um tipo de licença para Linux no License Manager

Você pode usar o License Manager Console ou o AWS CLI para converter o tipo de licença de Ubuntu LTS, RHEL e RHEL elegíveis para instâncias SAP.

Tópicos

Como converter um tipo de licença usando o console do License Manager

Você pode usar o console do License Manager para converter um tipo de licença.

> **Note**
>
> Somente as instâncias em estado interrompido e associadas pelo Inventário do AWS Systems Manager são exibidas.

Para iniciar uma conversão de tipo de licença no console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, escolha Conversão de tipo de licença e, em seguida, escolha Criar conversão de tipo de licença.
3. Em Sistema operacional de origem, escolha a plataforma da instância que você deseja converter:
   - RHEL
   - RHEL para SAP
   - Ubuntu LTS
   - BYOL do Windows
   - Windows com licença incluída
4. (Opcional) Filtre as instâncias disponíveis especificando um valor para o ID da instância ou para ovalor da operação de uso.
5. Selecione as instâncias cujas licenças você deseja converter e escolha Avançar.
6. Insira o valor da operação de uso para o tipo de licença, selecione a licença para a qual você está convertendo e escolha Avançar.
7. Verifique se está satisfeito com a configuração da conversão de tipo de licença e escolha Iniciar conversão.

Você pode ver o status da conversão de tipo de licença no painel correspondente. A coluna “Status da conversão” exibe o status da conversão, como Em andamento, Concluída ou Com falha.

Converta um tipo de licença usando o AWS CLI

Para iniciar uma conversão do tipo de licença no AWS CLI, você deve confirmar se o tipo de licença da sua instância está qualificado e, em seguida, realizar uma conversão do tipo de licença para mudar para a assinatura necessária. Para obter mais informações sobre os tipos de assinatura elegíveis, consulte Tipos de assinatura elegíveis para Linux no License Manager.

Determine o tipo de licença da instância

Verifique se você instalou e configurou o AWS CLI. Para obter mais informações, consulte Instalando, atualizando e desinstalando o AWS CLI e Configurando o. AWS CLI

> **Important**
>
> Talvez seja necessário atualizar o AWS CLI para executar determinados comandos e receber todas as saídas necessárias nas etapas a seguir. Verifique se você tem permissões para executar o `create-license-conversion-task-for-resource` AWS CLI comando. Para obter mais informações, consulte Criar políticas do IAM para o License Manager.

Para determinar o tipo de licença atualmente associado à sua instância, execute o AWS CLI comando a seguir. Substitua o ID da instância pelo ID da instância cujo tipo de licença você quer determinar:

```
aws ec2 describe-instances --instance-ids <instance-id> --query
 "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
 PlatformDetails, UsageOperation: UsageOperation, UsageOperationUpdateTime:
 UsageOperationUpdateTime}"
```

O seguinte é um exemplo de resposta ao comando `describe-instances`. O UsageOperationvalor é o código de informações de cobrança associado à licença. Um valor de operação de uso “`RunInstances`” indica que a instância está usando o licenciamento fornecido pela AWS . `UsageOperationUpdateTime` é a hora em que o código de faturamento foi atualizado. Para obter mais informações, consulte DescribeInstances na Referência de API do Amazon EC2.

```
"InstanceId": "i-0123456789abcdef",
```

```
"Platform details": "Linux/UNIX",
"UsageOperation": "RunInstances",
"UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
```

Conversões compatíveis com Red Hat

As seguintes conversões são suportadas para produtos Red Hat Enterprise Linux (RHEL). Cada conversão requer contextos específicos de licença de origem e destino e pode ter requisitos adicionais.

Conversão de RHEL para SAP com HA e serviços de atualização (vendido pela AWS in AWS Marketplace) para RHEL para SAP com HA e serviços de atualização (vendido pela Red Hat em) AWS Marketplace

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
 "UsageOperation=RunInstances:0010,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<so
 \
  --destination-license-context
 "UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<de
```

Observações:

- O RHEL for SAP com HA e Update Services (vendido pela AWS in AWS Marketplace) tem muitos códigos de produto diferentes IDs (também conhecidos como código do Marketplace), dependendo da assinatura AWS Marketplace do produto. Verifique a resposta de describe-instances do EC2 para obter o ID correto do código do produto em suas instâncias.
- O RHEL for SAP com HA e serviços de atualização (vendido pela Red Hat em AWS Marketplace) tem dois códigos de produto diferentes IDs: du6111oq9lwrc996awt04qyql (NA e Global) e 952qwcsxkm430zxhpy32i7w8g (EMEA). O que você deve usar depende da sua região. Verifique sua assinatura do RHEL for SAP com HA e Update Services no Marketplace para descobrir qual é.

Depois de convertida, você não pode converter a instância novamente em RHEL for SAP com HA e Update Services (Sold by AWS in AWS Marketplace), a menos que esteja na lista de permissões para esse recurso privado, que exige uma Suporte solicitação. Para obter mais informações, consulte Criar um caso de suporte.

Conversão de RHEL para SAP com HA e serviços de atualização (vendidos pela AWS in AWS Marketplace) em Red Hat Subscriptions (vendidas pela Red Hat in) AWS Marketplace

As assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) se referem às assinaturas SaaS das quais os clientes podem comprar. AWS Marketplace Também há duas listagens no momento.

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
 "UsageOperation=RunInstances:0010,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<so
 \
  --destination-license-context "UsageOperation=RunInstances:00g0"
```

Observações:

- O RHEL for SAP com HA e Update Services (vendido pela AWS in AWS Marketplace) tem muitos códigos de produto diferentes IDs (também conhecidos como código do Marketplace), dependendo da assinatura AWS Marketplace do produto. Verifique a resposta de describe-instances do EC2 para obter o ID correto do código do produto em suas instâncias.
- As assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) não têm um código de produto para adicionar às instâncias.
  - Explicações: os códigos de produto SaaS não estão anexados às instâncias do EC2, portanto, espera-se que os clientes não incluam um código de produto de destino ao invocar create-license-conversion-task o comando da CLI -for-resource.

Depois de convertida, você não pode converter a instância novamente em RHEL for SAP com HA e Update Services (Sold by AWS in AWS Marketplace), a menos que esteja na lista de permissões para esse recurso privado, que exige uma Suporte solicitação. Para obter mais informações, consulte Criar um caso de suporte.

Conversão de Red Hat License-Included (LI) para RHEL (vendido pela Red Hat em) AWS Marketplace

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
```

```
  --resource-arn <instance_arn> \
  --source-license-context "UsageOperation=RunInstances:0010" \
  --destination-license-context
 "UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<de
```

Observações:

- O RHEL (vendido pela Red Hat em AWS Marketplace) tem dois códigos de produto diferentes IDs: 6cd5fxzrad0cu2j23p692xytz (NA e Global) e 6t1yup6mik9ng3ge36n33xqhw (EMEA). O que você deve usar depende da sua região. Verifique sua assinatura do RHEL for SAP com HA e Update Services no Marketplace para descobrir qual é.

Conversão de Red Hat Enterprise Linux (RHEL) AWS para Red Hat License-Included (LI)

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
 "UsageOperation=RunInstances,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<source_
 \
  --destination-license-context "UsageOperation=RunInstances:0010"
```

Ou esse:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
 "UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<so
 \
  --destination-license-context "UsageOperation=RunInstances:0010"
```

Observações:

- O Red Hat Enterprise Linux (RHEL) for AWS tem dois códigos de produto diferentes IDs: 6cd5fxzrad0cu2j23p692xytz (NA e Global) e 6t1yup6mik9ng3ge36n33xqhw (EMEA). O que você deve usar depende da sua região. Verifique a resposta de describe-instances do EC2 para obter o ID correto do código do produto em suas instâncias.
- O Red Hat Enterprise Linux (RHEL) para AWS instâncias pode ter operação de uso RunInstances RunInstances or:00g0. Isso depende se as instâncias foram originalmente lançadas a partir de

um Red Hat Enterprise Linux (RHEL) para AMI de AWS produto ou se foram posteriormente convertidas nessa assinatura. Verifique a resposta de describe-instances do EC2 para ver a operação de uso correta em suas instâncias.

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context "UsageOperation=RunInstances:0010" \
  --destination-license-context "UsageOperation=RunInstances:00g0"
```

Observações:

- As assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) não têm um código de produto para adicionar às instâncias.
  - Explicações: os códigos de produto SaaS não estão anexados às instâncias do EC2, portanto, espera-se que os clientes não incluam um código de produto de destino ao invocar create-license-conversion-task o comando da CLI -for-resource.
- As assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) devem ser assinadas pelo chamador do comando CLI. Ainda não há suporte para assinaturas em outras contas na mesma organização.

Conversão de assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) para Red Hat License-Included (LI)

Exemplo de comando da CLI:

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context "UsageOperation=RunInstances:00g0" \
  --destination-license-context "UsageOperation=RunInstances:0010"
```

Observações:

- As assinaturas Red Hat (vendidas pela Red Hat em AWS Marketplace) não têm um código de produto adicionado às instâncias.

Outros requisitos

As instâncias devem estar paradas antes de criar suas tarefas de conversão de licenças. Os clientes não devem tentar iniciar ou encerrar as instâncias antes que as tarefas de conversão da licença sejam concluídas ou falhem. Esse é o mesmo requisito para todas as conversões de tipo de licença.

Se o destino for um desses produtos do Marketplace:

- RHEL para SAP com HA e serviços de atualização (vendido pela Red Hat em AWS Marketplace)
- RHEL (vendido pela Red Hat em AWS Marketplace)
- Assinaturas Red Hat (vendidas pela Red Hat em) AWS Marketplace

Em seguida, o cliente deve ter uma assinatura ativa no Marketplace antes de invocar o comando CLI. Caso contrário, a solicitação de conversão poderá ser rejeitada ou falhar. Diferentemente do Console, ao criar tarefas de conversão de licenças a partir da CLI, o License Manager não tenta inscrever automaticamente os clientes nos produtos de destino.

Como converter para Ubuntu Pro

Antes de converter sua instância do Ubuntu LTS para o Ubuntu Pro, sua instância deve ter acesso de saída à Internet configurado para recuperar um token de licença dos servidores da Canonical e instalar o Ubuntu Pro Client. Para obter mais informações, consulte Pré-requisitos de conversão para os tipos de licença do License Manager.

Para converter o Ubuntu LTS para o Ubuntu Pro, siga estas etapas:

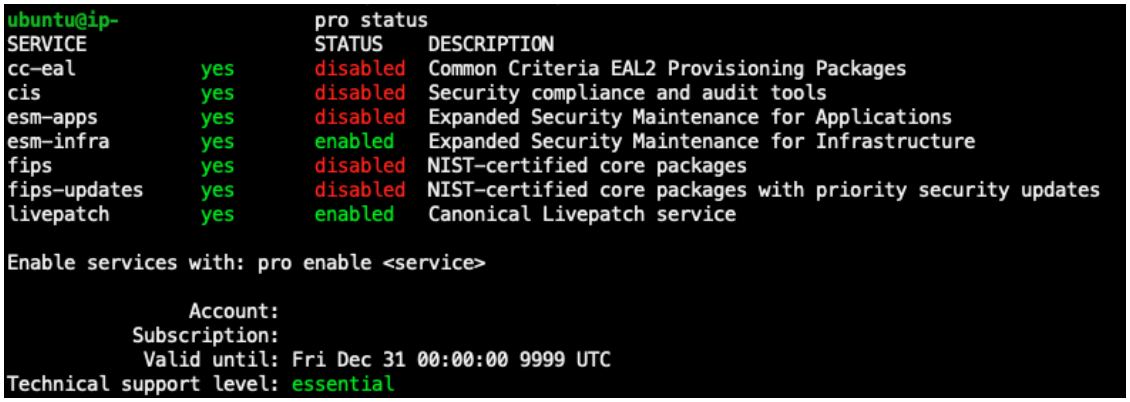
1. Execute o comando a seguir a partir do AWS CLI enquanto especifica o ARN da sua instância:

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances \
    --destination-license-context UsageOperation=RunInstances:0g00
```

2. Execute o comando a seguir de dentro da instância para recuperar detalhes sobre o status da sua assinatura do Ubuntu Pro:

```
pro status
```

3. Confirme se sua saída indica que a instância tem uma assinatura válida do Ubuntu Pro:



Como remover uma assinatura do Ubuntu Pro

A Conversão de tipo de licença só pode ser usada para converter do Ubuntu LTS para o Ubuntu Pro. Para converter do Ubuntu Pro para o Ubuntu LTS, faça uma solicitação para o Suporte. Para obter mais informações, consulte Criar um caso de suporte.

Conversão de locação no License Manager

Você pode alterar a locação da instância para melhor se adequar ao seu caso de uso. Você pode usar o modify-instance-placement AWS CLI comando para alternar entre as seguintes locações:

- Compartilhada
- Instância Dedicada
- Host Dedicado
- Grupos de atributos de host

Sua conta deve ter um host dedicado com capacidade disponível para iniciar a instância se você quiser mudar para o tipo de locação “Host Dedicado”. Para obter mais informações sobre o trabalho com Hosts Dedicados, consulte Como trabalhar com Hosts Dedicados no Guia do usuário do Amazon Elastic Compute Cloud.

Para migrar para o tipo de locação de grupos de recursos de host, você deve ter pelo menos um grupo de recursos de host na conta. Para iniciar uma instância em um grupo de recursos de host, a instância deve ter o mesmo conjunto de licenças associadas ao grupo de recursos de host. Para obter mais informações, consulte Hospede grupos de recursos no License Manager.

Limites de conversão de locação

Os limites a seguir se aplicam à conversão de locação:

- O código de faturamento do Linux é permitido em todos os tipos de locação.
- O código de faturamento Windows BYOL não é permitido na locação “Compartilhada”.
- O código de faturamento do Windows Server com licença incluída é permitido em todos os tipos de locação.
- Todas as edições suportadas do SQL Server e a licença SUSE (SLES), incluindo códigos de cobrança, são permitidos em locação compartilhada e instâncias dedicadas. No entanto, esses códigos de faturamento não são permitidos em Hosts dedicados e grupos de recursos de host.
- Com exceção do Windows Server, códigos de faturamento com licença incluída não são permitidos em Hosts dedicados e grupos de recursos de host.

Alterar a locação de uma instância usando o AWS CLI

Uma instância deve estar no estado `stopped` para ter sua locação alterada.

Para interromper a instância, execute o seguinte comando:

```
aws ec2 stop-instances --instance-ids <instance_id>
```

Para alterar uma instância de qualquer locação para as locações `default` ou `dedicated`, execute os seguintes comandos:

`default`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy default
```

`dedicated`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy dedicated
```

Para alterar uma instância de qualquer locação para a locação `host` com posicionamento automático, execute o seguintes comando:

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
```

```
  --tenancy host --affinity default
```

Para alterar uma instância de qualquer locação para a locação `host`, segmentando um Host Dedicado específico, execute o seguinte comando:

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --affinity host --host-id <host_id>
```

Para alterar uma instância de qualquer locação para a locação `host` usando um Grupo de atributos de Host, execute o seguinte comando:

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --host-resource-group-arn <host_resource_group_arn>
```

Solução de problemas de conversão de tipo de licença no License Manager

Tópicos de solução de problemas

- Ativação do Windows
- A instância [instância] é executada a partir de uma AMI de propriedade da Amazon. Forneça uma instância iniciada originalmente a partir de uma AMI BYOL.
- Falha ao validar que a instância [instância] foi executada a partir de uma AMI BYOL. Certifique-se de que o SSM Agent está em execução na instância.
- Ocorreu um erro (InvalidParameterValueException) ao chamar a CreateLicenseConversionTaskForResource operação: ResourceId - [instance] está em um estado inválido para alterar o tipo de licença.
- A instância [instância] do EC2 falhou ao ser interrompida. Verifique se você tem permissões para EC2 StopInstances.

Ativação do Windows

Uma conversão de tipo de licença contém várias etapas. Em alguns casos, quando você converte instâncias do Windows Server de BYOL para a licença incluída, os produtos de faturamento em uma instância são atualizados com êxito. No entanto, o servidor KMS pode não mudar para o servidor KMS da AWS .

Para corrigir esse problema, siga as etapas em Por que a ativação do Windows falhou na minha instância EC2 do Windows? Assim, você pode ativar o Windows com o Automation runbook

AWSSupport-ActivateWindowsWithAmazonLicense do Systems Manager ou fazer login na instância e alterar manualmente para o servidor KMS da AWS .

A instância [instância] é executada a partir de uma AMI de propriedade da Amazon. Forneça uma instância iniciada originalmente a partir de uma AMI BYOL.

Você deve iniciar sua instância do Amazon EC2 Windows a partir de uma AMI importada para realizar uma conversão de tipo de licença para o modelo Traga sua própria licença (BYOL). Instâncias originalmente lançadas a partir de uma AMI de propriedade da Amazon não estão qualificadas para conversão para BYOL. Para obter mais informações, consulte Pré-requisitos de conversão para os tipos de licença do License Manager.

Falha ao validar que a instância [instância] foi executada a partir de uma AMI BYOL. Certifique-se de que o SSM Agent está em execução na instância.

Para que a Conversão de tipo de licença seja bem-sucedida, sua instância deve primeiro estar on-line e ser gerenciada pelo Systems Manager para que o inventário seja coletado. O AWS Systems Manager Agent (SSM Agent) reunirá o inventário da sua instância, que inclui detalhes sobre o sistema operacional. Para obter mais informações, consulte Verificar o status do SSM Agent e iniciar o agente e Solução de problemas do SSM Agent no Guia do Usuário do AWS Systems Manager .

Ocorreu um erro (InvalidParameterValueException) ao chamar a **`CreateLicenseConversionTaskForResource`** operação: ResourceId - [instance] está em um estado inválido para alterar o tipo de licença.

Para realizar uma conversão de tipo de licença, a instância de destino deve estar no estado interrompido. Para obter mais informações, consulte Pré-requisitos de conversão para os tipos de licença do License Manager e Solução de problemas na interrupção da instância no Guia do usuário do Amazon Elastic Compute Cloud.

A instância [instância] do EC2 falhou ao ser interrompida. Verifique se você tem permissões para EC2 **`StopInstances.`**

Você deve ter permissões para realizar a API `StopInstances` do EC2 na instância de destino. Se a proteção contra interrupção estiver ativada na instância de destino, o processo de conversão falhará. Para obter mais informações, consulte Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida no Guia do usuário do Amazon Elastic Compute Cloud.

Hospede grupos de recursos no License Manager

Os Amazon EC2 Dedicated Hosts são servidores físicos com capacidade de EC2 instância totalmente dedicada ao seu uso. Um grupo de atributos de host é uma coleção de Hosts Dedicados gerenciados como uma única entidade. Conforme você executa instâncias, o License Manager aloca os hosts e executa instâncias neles com base nas configurações que você definiu. Você pode adicionar Hosts Dedicados existentes a um grupo de atributos de host e aproveitar o gerenciamento automatizado de hosts por meio do License Manager. Para obter mais informações, consulte Hosts dedicados no Guia EC2 do usuário da Amazon.

Você pode usar esses grupos de recursos de host para separar hosts por finalidade. Por exemplo, hosts de teste de desenvolvimento versus produção, unidade organizacional ou restrição de licença. Depois de adicionar um Host Dedicado a um grupo de recursos de host, você não pode executar instâncias diretamente no Host Dedicado. Execute-as usando o grupo de recursos de host.

Configurações

Você pode definir as seguintes configurações para um grupo de recursos de host:

- Alocar hosts automaticamente — Indica se a Amazon EC2 pode alocar novos hosts em seu nome se o lançamento de uma instância nesse grupo de recursos de host exceder sua capacidade disponível.
- Liberar anfitriões automaticamente — Indica se a Amazon EC2 pode liberar anfitriões não utilizados em seu nome. Um host não utilizado não tem instâncias em execução.
- Recupere hosts automaticamente — Indica se a Amazon EC2 pode mover instâncias de um host que falhou inesperadamente para um novo host.
- Licenças autogerenciadas associadas — As licenças autogerenciadas que podem ser usadas para executar instâncias nesse grupo de atributos de host.
- (Opcional) Famílias de instâncias — Os tipos de instâncias que você pode executar. Por padrão, você pode executar qualquer tipo de instância compatível com um Host Dedicado. Se você executar instâncias baseadas em Nitro, poderá executar instâncias de diferentes tipos no mesmo grupo de recursos de host. Caso contrário, você deverá executar somente instâncias do mesmo tipo no mesmo grupo de recursos de host.

Conteúdo

- Compartilhe um grupo de recursos do host no License Manager
- Adicionar hosts dedicados a um grupo de recursos de host no License Manager
- Execute uma instância em um grupo de recursos do host no License Manager
- Modificar um grupo de recursos do host no License Manager
- Remover hosts dedicados de um grupo de recursos de host no License Manager
- Excluir um grupo de recursos do host no License Manager

Crie um grupo de recursos do host no License Manager

Configure um grupo de recursos de host para permitir que o License Manager gerencie seus hosts dedicados. Para melhor utilizar suas licenças mais caras, associe uma ou mais licenças autogerenciadas baseadas em núcleo ou soquete ao grupo de recursos de host. Para otimizar a utilização de hosts, você pode permitir todas as licenças autogerenciadas baseadas em núcleo ou soquete no grupo.

Como criar um grupo de atributos de host

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Escolha Criar grupo de atributos de host.
4. Para Detalhes do grupo de recursos de hosts, especifique um nome e uma descrição para o grupo de recursos de host.
5. Para configurações de gerenciamento de host EC2 dedicado, ative ou desative as seguintes configurações conforme necessário:
   - Alocar hosts automaticamente
   - Liberar hosts automaticamente
   - Recuperar hosts automaticamente
6. (Opcional) Para Configurações adicionais, selecione as famílias de instâncias que podem ser executadas no grupo de recursos de host.
7. Para licenças autogerenciadas, selecione uma ou mais licenças autogerenciadas baseadas em núcleo ou soquete.
8. (Opcional) Para Tags, adicione uma ou mais tags.
9. Escolha Criar.

Compartilhe um grupo de recursos do host no License Manager

Você pode usar AWS Resource Access Manager para compartilhar seus grupos de recursos anfitriões por meio de AWS Organizations. Depois de compartilhar um grupo de recursos de host e uma licença autogerenciada, as contas de membro podem executar instâncias no grupo compartilhado. Os novos hosts são alocados na conta proprietária do grupo de recursos de host. A conta-membro é proprietária das instâncias. Para obter mais informações, consulte o Guia do usuário do AWS RAM.

Adicionar hosts dedicados a um grupo de recursos de host no License Manager

Você pode adicionar seus hosts existentes a um grupo de recursos de host a partir da AWS API Console de gerenciamento da AWS AWS CLI,, ou. Para adicionar seus anfitriões, você deve ser o proprietário da AWS conta na qual criou o host dedicado e os grupos de recursos do host. Se seu grupo de recursos de host lista licenças autogerenciadas e tipos de instância, o host adicionado precisará ter estes requisitos.

> **Note**
>
> Se você interromper as instâncias e quiser reiniciá-las, deverá realizar as duas tarefas a seguir:
>
> - Modifique a instância para que ela aponte para o grupo de recursos de host.
> - Associe licenças autogerenciadas para corresponder ao grupo de recursos de host.

Não há limite para o número de hosts dedicados que você pode adicionar a um grupo de recursos de host. Para obter mais informações sobre Grupos de atributos, consulte o Guia do Usuário do Grupos de recursos da AWS.

Siga as etapas a seguir para adicionar um ou mais Hosts dedicados a um grupo de atributos:

1. Faça login no console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Grupo de atributos de host.
3. Na lista de nomes do grupo de recursos de host, clique no nome do grupo de recursos do host onde o Host Dedicado será adicionado.

4. Escolha Hosts dedicados.
5. Escolha Adicionar.
6. Escolha um ou mais Hosts dedicados para adicionar ao grupo de recursos de host.
7. Escolha Adicionar.

   Adicionar o host pode levar de 1 a 2 minutos. Em seguida, ele aparece na lista de Hosts Dedicados.

Execute uma instância em um grupo de recursos do host no License Manager

Ao executar uma instância, você pode especificar um grupo de recursos de host. Por exemplo, você pode executar o comando run-instances. É necessário associar uma licença autogerenciada baseada em núcleo ou soquete à AMI.

```
aws ec2 run-instances --min-count 2 --max-count 2 \
--instance-type c5.2xlarge --image-id ami-0abcdef1234567890 \
--placement="Tenancy=host,HostResourceGroupArn=arn"
```

Você também pode usar o EC2 console da Amazon. Para obter mais informações, consulte Lançamento de instâncias em um grupo de recursos do host no Guia EC2 do usuário da Amazon.

Modificar um grupo de recursos do host no License Manager

É possível modificar as configurações de um grupo de recursos de host a qualquer momento. O limite de host não pode ficar abaixo do número de hosts existentes no grupo de recursos de host. Você não pode remover um tipo de instância se houver uma instância desse tipo em execução no grupo de recursos de host.

Como modificar um grupo de atributos de host

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Selecione o grupo de recursos de host e escolha Ações, Editar.
4. Modifique as configurações conforme necessário.
5. Escolha Salvar alterações.

Remover hosts dedicados de um grupo de recursos de host no License Manager

Quando você remove um host do grupo, a instância em execução nesse host permanece nele. As instâncias anexadas ao grupo de recursos de host permanecem associadas ao grupo, e as instâncias diretamente anexadas ao host por afinidade mantêm a mesma propriedade. Se você compartilhar o grupo de recursos do host com outras AWS contas, o License Manager removerá automaticamente o host compartilhado e os consumidores receberão um aviso de despejo para mover suas instâncias do host em 15 dias. Para trabalhar com um host dedicado que foi removido de um grupo de recursos de host, consulte Trabalhar com hosts dedicados no Guia EC2 do usuário da Amazon.

Siga as etapas a seguir para adicionar um Host dedicado de um grupo:

1. Faça login no console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Grupo de atributos de host.
3. Clique no nome do atributo de host do qual você deseja remover um Host Dedicado.
4. Escolha Hosts Dedicados.
5. Escolha o Host dedicado a ser excluído do grupo. Você também pode pesquisar um Host Dedicado por ID, tipo, estado ou zona de disponibilidade.
6. Escolha Remover.
7. Escolha Remover novamente para confirmar.

Excluir um grupo de recursos do host no License Manager

Você poderá excluir um grupo de recursos de host se ele não tiver hosts.

Como excluir um grupo de atributos de host

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Selecione o host e escolha Ações, Excluir.
4. Quando a confirmação for solicitada, escolha Excluir.

Use assinaturas baseadas no usuário do License Manager para produtos de software compatíveis

Com as assinaturas baseadas no usuário AWS License Manager, você pode comprar assinaturas de software licenciado totalmente compatíveis. As licenças são fornecidas pela Amazon e têm uma taxa de assinatura baseada no usuário. O Amazon EC2 fornece Imagens de máquina da Amazon (AMIs) pré-configuradas com o software compatível e com as licenças do Windows Server incluídas. As licenças podem ser usadas sem compromisso de licenciamento de longo prazo.

Para usar assinaturas baseadas em usuário, você associa usuários de AWS Directory Service for Microsoft Active Directory(AWS Managed Microsoft AD) ou do seu domínio autogerenciado (local) às instâncias do EC2 que fornecem o software. Para disponibilizar o software licenciado, devem ser criadas assinaturas baseadas no usuário e associá-las a instâncias inicializadas a partir de AMIs pré-configuradas. O AWS Systems Manager configura e fortalece as instâncias incluídas na licença executada. Os usuários devem se conectar ao software Remote Desktop para acessar as instâncias que fornecem o software.

Incorrem cobranças para cada usuário e vCPU associados às instâncias incluídas na licença. Os modelos de preços das Instâncias Reservadas e Savings Plans do Amazon EC2 ajudam a otimizar os custos do Amazon EC2. Para obter mais informações, consulte Instâncias reservadas no Guia do usuário do Amazon Elastic Compute Cloud. User-based as assinaturas são cobradas da primeira metade do mês até o final do mês.

Tópicos

- Execute uma instância a partir de uma licença incluída (AMI)
- Conecte-se a uma instância de assinatura baseada em usuário com o RDP
- Modifique as configurações de firewall para sua assinatura do Microsoft Office
- Gerencie usuários de assinatura para assinaturas baseadas em usuários do License Manager
- Cancelar o registro de um Active Directory nas configurações do License Manager
- Solucionar problemas de assinaturas baseadas em usuário no License Manager

Considerações sobre o uso de assinaturas baseadas em usuário no License Manager

As considerações a seguir se aplicam ao usar assinaturas baseadas em usuário com o License Manager:

- A AWS Marketplace assinatura do Microsoft Remote Desktop Services (`Win Remote Desktop Services SAL`) com licença incluída tem uma taxa mensal por usuário, sem rateio.
- Por padrão, as instâncias que fornecem assinaturas baseadas no usuário oferecem suporte a até duas sessões ativas de usuário por vez. Para habilitar mais de duas sessões de usuário ativas, você pode configurar um Objeto de Política de Grupo (GPO) do Active Directory e definir o modo de licenciamento do Microsoft RDS como. `Per User` Para obter mais informações, consulte os pré-requisitos para. Configurar o GPO do Active Directory para sessões de usuário remoto mais ativas
- Quando você cria usuários locais com privilégios de administrador em instâncias que fornecem assinaturas baseadas em usuários, o status de integridade da instância pode mudar para não íntegro. O License Manager pode terminar instâncias que não estejam íntegras devido à não conformidade. Para obter mais informações, consulte Solucionar problemas de não conformidade de uma instância.
- Quando você configura seu Active Directory com produtos do Microsoft Office, sua VPC deve ter endpoints de VPC provisionados em pelo menos uma sub-rede. Se quiser remover todos os recursos de VPC endpoint criados pelo License Manager, você deve remover qualquer Active Directory que esteja configurado nas configurações do License Manager. Para obter mais informações, consulte Cancelar o registro de um Active Directory nas configurações do License Manager.
- A chave de tag de `AWSLicenseManager` com o valor de `UserSubscriptions` atribuído pelo License Manager às suas instâncias não deve ser alterada nem excluída.

- Para que o serviço funcione conforme o esperado, as duas interfaces de rede criadas para o License Manager não devem ser alteradas ou excluídas.
- Os objetos que o License Manager cria na unidade organizacional AWS reservada (OU) do AWS Managed Microsoft AD diretório não devem ser alterados nem excluídos.
- As instâncias implantadas para assinaturas baseadas no usuário devem ser nós gerenciados por AWS Systems Manager e ingressar no mesmo domínio. Para obter informações sobre como manter as instâncias gerenciadas pelo Systems Manager, consulte a seção Solucionar problemas de assinaturas baseadas em usuário no License Manager deste guia.
- Para parar de incorrer em cobranças de assinatura do Microsoft Office ou do Visual Studio para um usuário, você deve desassociar o usuário de todas as instâncias às quais ele está associado. Para obter mais informações, consulte Desassociar usuários de uma instância que fornece assinaturas baseadas no usuário do License Manager.

Cobranças de assinatura no License Manager

A assinatura e o faturamento no License Manager variam de acordo com o produto de assinatura usado.

Assinaturas do Microsoft Office e do Visual Studio

Para assinaturas do Microsoft Office e do Visual Studio, o faturamento é interrompido assim que você desassocia o usuário de todas as instâncias que fornecem o produto por assinatura e cancela a assinatura do produto.

Assinaturas do Microsoft Remote Desktop Services (RDS)

O Microsoft RDS é cobrado por usuário, por mês, com base em uma combinação da assinatura do usuário e do token da licença de acesso do cliente (CAL) emitido pelo servidor de licenças quando o usuário se conecta a uma instância que fornece o produto de assinatura.

Cobrança do Microsoft RDS no License Manager

A cobrança do Microsoft RDS começa quando o usuário do Active Directory é inscrito por meio do License Manager e termina após a expiração do token da licença de acesso para cliente (CAL), 60 dias a partir da data de emissão, sem rateio por meses parciais. O faturamento continua até que o token expire, mesmo se você cancelar a assinatura do usuário.

Se um usuário não inscrito continuar fazendo login após a expiração do token de licença, ele será automaticamente inscrito novamente e o faturamento continuará até que a assinatura seja cancelada novamente e seu token expire.

Da mesma forma, se um usuário que nunca se inscreveu, mas fizer login em uma instância associada ao servidor de licenças, o License Manager o inscreverá automaticamente e iniciará o faturamento do RDS. O faturamento continua até que a assinatura seja cancelada e o token expire.

Para interromper a cobrança de um usuário no final do mês atual, você deve remover esse usuário do Active Directory que está configurado para o servidor de licenças antes de cancelar a assinatura.

> **Warning**
>
> Se você remover um usuário do Active Directory que ainda tenha uma assinatura ativa do Microsoft Office ou do Visual Studio, esse usuário não poderá mais acessar as instâncias às quais está associado.

Os exemplos de cenários a seguir demonstram como o faturamento do RDS funciona.

Cenário 1: assinatura e cobrança padrão

O cenário a seguir mostra um conjunto padrão de ações que afetam a cobrança de um usuário do Active Directory (AD) que está inscrito em 12/15 /2024, mas nunca acessa uma instância de assinatura.

Ação: Se o usuário nunca cancelar a assinatura, a cobrança continuará indefinidamente.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
12/15/2024	12/15/2024	--	N/A	--	--	--

Ação: O usuário não está inscrito em /2025. 1/15

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
12/15/2024	12/15/2024	--	N/A	1/15/2025	No	1/31/2025

Cenário 2: como o token de licença afeta a assinatura e o faturamento do usuário

O cenário a seguir mostra como a expiração do token de licença afeta a assinatura do usuário de um usuário do Active Directory (AD) que está inscrito em 9/15 /2024 e faz login em uma instância de produto de assinatura associada ao domínio no mesmo dia.

Ação: Assinatura inicial e login para o usuário do AD.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

Ação: O mesmo usuário do AD não está inscrito em /2024. 10/19 No entanto, como o usuário não foi removido do diretório, a cobrança continua até o final do mês em que o token de licença expira.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

Ação alternativa: O administrador do AD remove o usuário do diretório em 10/20 /2024 e, em seguida, cancela a assinatura do usuário no dia seguinte. Nesse caso, o faturamento é interrompido no final do mês durante o qual o usuário é removido do diretório.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/21/2024	10/20/2024	10/31/2024

Cenário 3: O usuário não inscrito é inscrito novamente

O cenário a seguir mostra como um usuário não inscrito do Active Directory (AD) cujo token de licença expirou é automaticamente reinscrito quando acessa uma instância de produto de assinatura associada ao domínio.

Ação: Assinatura inicial e login para o usuário do AD.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

Ação: O mesmo usuário do AD não está inscrito em /2024. 10/19 No entanto, como o usuário não foi removido do diretório, a cobrança continua até o final do mês em que o token de licença expira.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

Ação: o mesmo usuário do AD acessa uma instância de produto de assinatura associada ao domínio após a expiração do token de licença anterior, mas antes do término do faturamento. O faturamento continua até que o usuário cancele a assinatura novamente e o novo token expire.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
11/20/2024 (re-subscribed)	billing continues	11/20/2024	1/20/2025	--	--	--

Cenário 4: assinatura automática no acesso à instância

O cenário a seguir mostra como um usuário do Active Directory (AD) que nunca foi inscrito no RDS SAL é automaticamente inscrito quando faz login em uma instância de produto de assinatura associada ao domínio.

Ação: um usuário do AD que nunca foi inscrito no RDS SAL faz login em uma instância de produto de assinatura associada ao domínio em 9/15 /2024 e é inscrito automaticamente. O faturamento começa e continua até que o usuário cancele a assinatura e seu novo token expire.

Usuário do AD inscrito	O faturamento começa	CAL emitida	A CAL expira	Usuário não inscrito	Usuário removido do AD	O faturamento termina
9/15/2024 (subscrição automática)	9/15/2024	9/15/2024	11/15/2024	--	--	--

Para obter mais informações sobre como as CALs por usuário do Microsoft RDS funcionam, consulte a seção CALs por usuário no artigo Licenciar sua implantação de área de trabalho remota no site do Microsoft Learn.

Pré-requisitos para criar assinaturas baseadas no usuário no License Manager

Os pré-requisitos a seguir devem estar implementados no ambiente antes que seja possível criar assinaturas baseadas no usuário.

Sumário

Funções e permissões do IAM

Você deve permitir que o License Manager crie um perfil vinculado ao serviço para integrar as assinaturas da sua Conta da AWS para usuários. No console do License Manager, uma solicitação aparece nas User-based assinaturas se a função ainda não tiver sido criada. Depois de responder à solicitação e concordar em permitir que o License Manager crie a função, escolha Create para continuar. Para obter mais informações, consulte Usando funções vinculadas a serviços para o License Manager.

Para criar assinaturas baseadas no usuário, o usuário ou perfil deve ter as seguintes permissões:

- Amazon EC2 — Trabalhe com interfaces de rede e sub-redes.
  - `ec2:CreateNetworkInterface`
  - `ec2:DeleteNetworkInterface`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:CreateNetworkInterfacePermission`
  - `ec2:DescribeSubnets`
- Directory Service— Administrar Active Directories.

  - `ds:DescribeDirectories`
  - `ds:AuthorizeApplication`
  - `ds:UnauthorizeApplication`
  - `ds:GetAuthorizedApplicationDetails`
  - `ds:DescribeDomainControllers`
- Route 53 — Configurar o roteamento.
  - `route53:DeleteHealthCheck`
  - `route53:ChangeResourceRecordSets`
  - `route53:GetHostedZone`
  - `route53:ListHostedZonesByName`
  - `route53:ListHostedZones`
  - `route53:ListHostedZonesByVPC`
  - `route53:CreateHostedZone`
  - `route53:DeleteHostedZone`
  - `route53:ListResourceRecordSets`
  - `route53:GetHealthCheckCount`
  - `route53:AssociateVPCWithHostedZone`

Para criar assinaturas baseadas no usuário para produtos do Microsoft Office, o usuário ou perfil também deve ter as permissões adicionais a seguir:

- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`
- `ec2:DescribeSecurityGroups`

AWS KMS Política chave para credenciais do Servidor de Licenças

Para usar sua própria chave KMS para criptografar e descriptografar o segredo das credenciais administrativas do Microsoft RDS License Server, você deve anexar uma política à função que você usa para acessar as operações do License Manager. O exemplo a seguir mostra uma

política que concede permissão para o Secrets Manager acessar a chave KMS para criptografar e descriptografar o segredo da credencial do Microsoft RDS License Server.

JSON

```
{
"Version":"2012-10-17",
"Id": "key-policy",
"Statement": [
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/RoleName"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "secretsmanager.*.amazonaws.com"
            }
        }
    },
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/aws-
service-role/license-manager-user-subscriptions.amazonaws.com/
AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService"
        },
        "Action": "kms:Decrypt",
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "secretsmanager.*.amazonaws.com"
            }
        }
    }
```

```
]
}
```

Active Directory

Para usar as assinaturas baseadas no usuário do License Manager, você deve criar um Active Directory (AD) que contenha informações do usuário para os usuários do produto de assinatura. Dependendo da sua configuração, você pode usar um AWS Managed Microsoft AD AD ou um AD autogerenciado.

Se você usar diretórios ativos AWS gerenciados e autogerenciados, deverá estabelecer uma relação de confiança bidirecional entre os diretórios. Para obter mais informações, consulte Tutorial: Crie uma relação de confiança entre seu domínio autogerenciado do Active Directory AWS Managed Microsoft AD e o seu no Guia de AWS Directory Service Administração.

> **Note**
>
> As sub-redes configuradas para seu diretório devem ser todas da mesma VPC do seu. Conta da AWS Não há suporte para sub-redes compartilhadas.

AWS Os Active Directórios gerenciados têm as seguintes restrições.

- Os diretórios compartilhados com você só são suportados se o diretório for integrado primeiro na conta principal e, em seguida, você poderá integrá-lo em uma conta compartilhada.
- Multi-factor a autenticação não é suportada

Pré-requisito para filtros baseados em tags

Se você usar filtros baseados em tags para o Active Directory, primeiro deverá integrar-se ao Explorador de recursos da AWS serviço, da seguinte maneira:

1. Abra o console do Resource Explorer em https://resource-explorer.console.aws.amazon.com/resource-explorer.
2. Escolha Ativar o Explorador de Recursos.
3. Na página Configurar o Resource Explorer, escolha uma opção de configuração, da seguinte maneira.

Configuração Rápida

Selecione essa opção para configuração básica.

Configuração avançada

Selecione essa opção para configuração personalizada. Certifique-se de criar um índice para pelo menos a região em que seu Active Directory reside.

4. Selecione uma região para a região do índice agregador.
5. Escolha Ativar o Explorador de Recursos para salvar suas configurações.
6. No painel de navegação, selecione Exibições e, em seguida, escolha Criar exibição.

> **Note**
>
> Para mostrar o painel de navegação se ele estiver oculto, escolha o ícone do menu (três barras horizontais).

7. a. Na página Criar visualização, insira **`license-manager-user-subscriptions-view`** o Nome.
   b. Verifique se o filtro Recursos está definido para Incluir todos os recursos.
   c. Na seção Atributos adicionais de recursos, verifique se a caixa de seleção Tags está marcada.
8. Escolha Criar visualização para finalizar.

Para obter mais informações sobre como criar um AWS Managed Microsoft AD diretório, consulte os AWS Managed Microsoft AD pré-requisitos e Criar seu AWS Managed Microsoft AD diretório no Guia do AWS Directory Service usuário.

Para associar usuários a AWS Managed Microsoft AD, você deve provisionar usuários em seu AWS Managed Microsoft AD diretório. Para obter mais informações, consulte Gerenciar usuários e grupos no AWS Managed Microsoft AD no Guia de administração AWS Directory Service .

Grupos de segurança

Os grupos de segurança controlam o tráfego de rede que é permitido entrar e sair dos recursos em sua rede. Para garantir que os recursos em seu ambiente de assinatura baseado em usuário possam se comunicar, seus grupos de segurança devem atender aos seguintes critérios.

Grupo de segurança para VPC endpoints

Identifique ou crie um grupo de segurança que permita a conectividade da porta TCP de entrada. 1688 Ao definir suas configurações de VPC, você especificará esse grupo de segurança. Para obter mais informações, consulte Trabalhar com grupos de segurança.

O License Manager associa esse grupo de segurança aos endpoints da VPC que ele cria em seu nome ao configurar a VPC. Para obter mais informações, consulte Acessar um serviço da AWS por meio de um endpoint da VPC de interface no Guia de AWS PrivateLink .

Grupo de segurança para controladores de domínio do Active Directory

Certifique-se de que o grupo de segurança que você usa para seus controladores de domínio do AD permita tráfego de saída para o endereço IP da interface de rede de cada controlador de domínio. Além disso, o grupo de segurança do controlador de domínio deve permitir a comunicação em todas as portas relacionadas ao Active Directory, incluindo o TCP 9389. A porta 9389 é necessária para os Serviços Web do Active Directory (ADWS), que é usada pelo PowerShell módulo Active Directory e outras ferramentas de gerenciamento para se comunicar com controladores de domínio.

Requisitos de grupo de segurança para a etapa “Registrar seu Active Directory”

Durante a integração do Active Directory ao License Manager, criamos uma interface de rede nas sub-redes fornecidas, que é marcada com o grupo de segurança padrão da VPC. Certifique-se de que esse grupo de segurança tenha permissão para acessar seus controladores de domínio do Active Directory. Isso pode ser substituído por um grupo de sua escolha após a conclusão da integração, mas ainda exigirá acesso à rede para os controladores de domínio.

Requisitos de grupo de segurança para a etapa “Configurar servidor de licenças RDS”

Durante a configuração do servidor de licenças, o License Manager cria duas interfaces de rede nas sub-redes que você fornece. Essas interfaces de rede são automaticamente marcadas com um grupo de segurança recém-criado que inclui todas as configurações de porta necessárias. Certifique-se de que seus grupos de segurança do controlador de domínio do Active Directory permitam tráfego bidirecional dos CIDRs de sub-rede em todas as portas relacionadas ao Active Directory, incluindo a porta TCP 9389. A porta 9389 é necessária para os Serviços Web do Active Directory (ADWS), que é usada pelo PowerShell módulo Active Directory e outras ferramentas de gerenciamento para se comunicar com controladores de domínio.

Grupo de segurança para instâncias de assinatura baseadas em usuário

Identifique ou crie um grupo de segurança que permita o seguinte acesso de e para sua instância. Para obter mais informações, consulte Trabalhar com grupos de segurança.

- Conectividade de porta TCP de entrada de suas fontes de 3389 conexão aprovadas.
- 1688Conectividade de porta TCP de saída para alcançar os endpoints VPC e se comunicar com eles. AWS Systems Manager

Configuração de rede

O License Manager cria duas interfaces de rede que usam o grupo de segurança padrão da VPC em que a sua AWS Managed Microsoft AD está provisionada. Essas interfaces são usadas para que o serviço interaja com seu diretório. Para obter mais informações, consulte Etapa 2: Registrar seu Active Directory no License Manager e O que é criado no Guia de administração do AWS Directory Service .

Depois que o processo de provisionamento estiver concluído, você poderá associar um grupo de segurança diferente às interfaces criadas pelo License Manager.

Resolução do DNS

O Active Directory que você registrou para assinaturas baseadas em usuário deve ser acessível a partir de qualquer VPC e sub-rede que você tenha definido nas configurações do License Manager. Para garantir que os nós do Active Directory estejam acessíveis, configure a resolução de DNS da seguinte forma:

- Configure o encaminhamento de DNS entre as VPCs e os Active Directories que estão configurados nas configurações do License Manager para assinaturas baseadas no usuário. Você pode usar o Amazon Route 53 ou outro serviço DNS para encaminhamento de DNS. Para obter mais informações, consulte a postagem do blog Integrar a resolução de DNS do serviço de diretório com o Amazon Route 53 Resolvers.
- Habilitar os nomes de host DNS e a resolução DNS para a VPC. Para obter mais informações, consulte Visualizar e atualizar atributos DNS para a VPC.

Instâncias que fornecem produtos de assinatura baseados no usuário

Para que suas instâncias de assinatura baseadas em usuário funcionem conforme o esperado, você deve atender aos seguintes pré-requisitos:

- Configure um grupo de segurança para suas instâncias conforme descrito emGrupos de segurança.
- Certifique-se de que as instâncias executadas para fornecer assinaturas baseadas no usuário com o Microsoft Office tenham uma rota para a sub-rede em que os endpoints da VPC estão provisionados.
- As instâncias que fornecem assinaturas baseadas no usuário devem ser AWS Systems Manager gerenciadas para que tenham um status saudável. Além disso, suas instâncias devem ser capazes de ativar o licenciamento por assinatura baseado no usuário para permanecerem em conformidade após a ativação da licença.

> **Note**
>
> O License Manager tentará recuperar instâncias não íntegras, mas as instâncias que não puderem retornar ao status íntegro serão terminadas. Para obter informações sobre solução de problemas sobre como manter as instâncias gerenciadas pelo Systems Manager e sobre a conformidade das instâncias, consulte a seção Solucionar problemas de assinaturas baseadas em usuário no License Manager deste guia.

- É necessário ter uma função de perfil de instância associada às instâncias que fornecem os produtos de assinatura baseada no usuário que permite que o recurso seja gerenciado pelo AWS Systems Manager. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager no Guia do usuário do AWS Systems Manager .
- Você deve fazer Desassociar usuários de uma instância isso antes de encerrar a instância.

Serviços de desktop remoto da Microsoft

O servidor de licenças do Microsoft Remote Desktop Services requer um usuário administrativo definido no Active Directory associado. Esse usuário deve ser capaz de realizar as seguintes tarefas:

- Crie uma OU no domínio do Active Directory
- Instâncias de junção de domínio (criar computador) dentro da OU que é criada
- Adicionar um objeto de computador a um grupo de servidores de terminal dentro do domínio do Active Directory
- Tenha controle delegado para objetos de usuário no domínio do Active Directory para ler e gravar no servidor de licenças do Terminal Server, a fim de gerar relatórios do servidor de licenças.

Para saber mais sobre delegação, consulte Delegação de Controle nos Serviços de Domínio Active Directory.

Credenciais administrativas secretas

O License Manager usa AWS Secrets Manager para gerenciar as credenciais necessárias para tarefas de administração de usuários no servidor de licenças do Microsoft Remote Desktop Services. Antes de configurar o servidor de licenças, você deve criar um segredo no Secrets Manager que contenha as credenciais do usuário que executa tarefas de administração de usuários no servidor de licenças. Ao definir as configurações do servidor de licenças, você deve fornecer a ID do segredo que você criou.

> **Note**
>
> Esse deve ser o mesmo usuário que você definiu para a geração do relatório do servidor de licenças do RDS.

Para criar um segredo, siga as instruções detalhadas na página Criar um AWS Secrets Manager segredo no Guia do usuário do Secrets Manager, com as seguintes configurações específicas do License Manager.

> **Important**
>
> Para usar o segredo, o License Manager depende dos nomes exatos das chaves, do valor do nome de usuário e da chave de criptografia especificados na lista a seguir. O nome secreto deve começar com o seguinte prefixo:`license-manager-user-`.

Na página Escolher tipo de segredo:

- Tipo de segredo — Escolha outro tipo de segredo.
- Key/value pares — Especifique os seguintes pares de chaves para armazenar no segredo.

  Nome de usuário

  - Chave: `username`
  - Valor: `Administrator`

  Senha

  - Chave: `password`

    - Valor: *The password*
- Chave de criptografia — Para especificar uma chave KMS diferente da `aws/secretsmanager` chave, você deve anexar uma política à função que você usa para acessar as operações do License Manager. Para obter mais informações, consulte Funções e permissões do IAM.

Na página Configurar segredo:

- Nome secreto — Especifique um nome para seu segredo que comece com o prefixo que o License Manager usa para identificar os segredos das credenciais do servidor de licenças. Por exemplo:

```
license-manager-user-admin-credentials
```

Essas instruções pressupõem que você esteja usando o Console de gerenciamento da AWS para criar seu segredo. O Guia do Usuário do Secrets Manager também inclui instruções detalhadas para outros métodos. Para obter mais informações sobre o Secrets Manager, consulte O que é o Secrets Manager. Para obter informações especificamente relacionadas aos custos, consulte Preços AWS Secrets Manager no Guia do Usuário do Secrets Manager.

Produtos de software compatíveis para assinaturas baseadas em usuário no License Manager

AWS License Manager oferece suporte a assinaturas baseadas em usuário para Microsoft Visual Studio e Microsoft Office. A utilização do software suportado é monitorada pelo License Manager. É necessária uma única assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota (RDS SAL) do Windows Server para que cada usuário acesse uma instância com licença incluída que fornece um produto de assinatura baseada no usuário. Para obter mais informações, consulte Comece com assinaturas baseadas em usuário no License Manager.

Plataformas de sistema operacional (SO) Windows compatíveis

Você pode encontrar AMIs do Windows que incluem produtos cobertos pela licença RDS SAL para as seguintes plataformas do sistema operacional Windows:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

Software com suporte para assinaturas baseadas no usuário

O License Manager oferece suporte ao licenciamento baseado no usuário com o software a seguir.

- Microsoft Visual Studio
- Microsoft Office
  - Componente Microsoft Office EC2 Image Builder

Microsoft Visual Studio

O Microsoft Visual Studio é um ambiente de desenvolvimento integrado (IDE) que permite aos desenvolvedores criar, editar, depurar e publicar aplicativos. As AMIs fornecidas pelo Microsoft Visual Studio incluem o AWS Toolkit for .NET Refactoring e o AWS Toolkit for Visual Studio.

Edições com suporte

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

A tabela a seguir detalha os nomes das assinaturas de software e o valor do produto associado usado para as operações da API de assinatura baseada no usuário do License Manager.

Nome da assinatura de software	Valor do produto
Visual Studio Enterprise 2022	`VISUAL_STUDIO_ENTERPRISE`
Visual Studio Professional 2022	`VISUAL_STUDIO_PROFESSIONAL`

Microsoft Office

O Microsoft Office é uma coleção de software desenvolvida pela Microsoft para vários casos de uso de produtividade, incluindo trabalhar com documentos, planilhas e apresentações de slides.

Edições com suporte

- Office LTSC Professional Plus 2021

- Escritório LTSC Professional Plus 2024
- Office LTSC Professional Plus 2021 de 32 bits (x86)
- Office LTSC Professional Plus 2024 32 bits (x86)
- Padrão LTSC de escritório 2021
- Padrão LTSC 2024 do Office
- Office LTSC Standard 2021 de 32 bits (x86)
- Office LTSC Standard 2024 32 bits (x86)

A tabela a seguir detalha os nomes das assinaturas de software e o valor do produto associado usado para as operações da API de assinatura baseada no usuário do License Manager.

Nome da assinatura de software	Valor do produto
Office LTSC Professional Plus 2021	`OFFICE_PROFESSIONAL_PLUS`
Escritório LTSC Professional Plus 2024	`OFFICE_PROFESSIONAL_PLUS`
Padrão LTSC de escritório 2021	`OFFICE_STANDARD`
Padrão LTSC 2024 do Office	`OFFICE_STANDARD`

Componente Microsoft Office EC2 Image Builder

Além das AMIs pré-configuradas, o Microsoft Office também está disponível como componentes do EC2 Image Builder.

Os componentes do Image Builder estão disponíveis tanto para o Microsoft Office LTSC Professional Plus quanto para o Microsoft Office LTSC Standard. Você pode configurar o ano e a arquitetura da versão para atender às suas necessidades.

Ano da versão suportada

- 2021

- 2024

Arquitetura compatível

- 32 bits
- 64 bits

Combine o Microsoft Office com outros softwares

Você pode usar os componentes do Microsoft Office Builder com o EC2 Image Builder para criar AMIs personalizadas que incluem o Microsoft Office junto com outros softwares.

Os componentes do Office Image Builder podem ser usados com qualquer uma das seguintes AMIs básicas:

- Sua própria AMI personalizada
- Uma AMI de assinatura baseada em usuário do Visual Studio
- Uma AMI básica do Windows Server

Você também pode incluir componentes adicionais do EC2 Image Builder em sua receita de imagem junto com o componente do Office. Por exemplo, você pode adicionar componentes que instalam as ferramentas, os agentes ou as configurações da sua organização para produzir uma AMI totalmente personalizada que inclua o Office e qualquer outro software de que seus usuários precisem.

Combine o Microsoft Office e o Microsoft Visual Studio em uma única instância

Você pode agrupar vários produtos licenciados em uma única Amazon Machine Image (AMI) usando pipelines do EC2 Image Builder criados por meio do License Manager. Por exemplo, você pode criar uma AMI que inclua o Visual Studio Professional 2022 e o Office LTSC Professional Plus 2024 e, em seguida, iniciar instâncias com todos os produtos pré-instalados e pré-licenciados. Para obter instruções passo a passo, consulte Execute uma instância com os produtos Microsoft Office e Microsoft Visual Studio

Active Directory

O License Manager oferece suporte a assinaturas baseadas em usuário para Microsoft Visual Studio, Microsoft Office e Licença de Acesso por Assinante de Serviços de Área de Trabalho Remota

(RDS SAL). Os produtos podem oferecer suporte a um Active Directory AWS Managed Microsoft AD ou a um diretório ativo autogerenciado que seja implantado em seu AWS ambiente ou tenha conectividade de rede com uma VPC em seu ambiente. AWS

Esta tabela indica quais tipos de Active Directory são suportados por cada produto de software quando usado com assinaturas baseadas em usuário:.

Produto de software	AWS Managed Microsoft AD	Self-managed ANÚNCIO
Microsoft Visual Studio	Compatível	Não compatível
Microsoft Office	Compatível	Não compatível
Produto RDS SAL	Compatível	Compatível

Software adicional

É possível instalar software adicional em suas instâncias que não estejam disponíveis como assinaturas baseadas no usuário. Instalações adicionais de software não são monitoradas pelo License Manager. Essas instalações devem ser realizadas usando a conta administrativa do Active Directory. Se você usa um AWS Managed Microsoft AD, a conta administrativa (Admin) é criada por padrão em seu diretório. Para obter mais informações, consulte Conta de administrador no Guia de administração do Directory Service .

Para instalar software adicional com a conta administrativa do Active Directory, você deve:

- Inscreva a conta administrativa no produto fornecido pela instância.
- Associe a conta administrativa à instância.
- Conecte-se à instância usando a conta administrativa para realizar a instalação.

Para obter mais informações, consulte Comece com assinaturas baseadas em usuário no License Manager.

Comece com assinaturas baseadas em usuário no License Manager

As etapas a seguir detalham como você pode começar a usar assinaturas baseadas no usuário. Essas etapas pressupõem que você já tenha implementado os pré-requisitos necessários. Para obter

mais informações, consulte o Pré-requisitos para criar assinaturas baseadas no usuário no License Manager.

Etapas

- Etapa 1: assinar um produto
- Etapa 2: Registrar seu Active Directory no License Manager
- Etapa 3: Configurar o servidor de licenças RDS
- Etapa 4: iniciar uma instância para fornecer assinaturas baseadas no usuário
- Etapa 5: associar usuários a uma instância de assinatura baseada em usuário

Etapa 1: assinar um produto

Os produtos da Microsoft, como o Office ou o Visual Studio, exigem uma assinatura ativa antes que você possa associar os usuários do Active Directory a uma instância que inclua esses produtos. Os produtos de assinatura que exibem o botão Inscrever-se no AWS Marketplace na coluna Status da assinatura do Marketplace ainda não estão inscritos.

Quando você assina um produto de assinatura baseado em usuário da Microsoft a partir do AWS Marketplace, o License Manager adiciona automaticamente uma assinatura do Microsoft Remote Desktop Services (RDS) à sua conta, se você ainda não tiver uma. O RDS é necessário para acessar remotamente os desktops gráficos e os aplicativos Windows baseados em assinatura em instâncias EC2 lançadas a partir da licença incluída. AMIs

Você pode assinar seus produtos diretamente no AWS Marketplace usando os seguintes links:

- Visual Studio Professional
- Visual Studio Enterprise
- Escritório LTSC Professional Plus
- Padrão LTSC de escritório
- Win Remote Desktop Services SAL

Descubra e assine produtos do console do License Manager

Você também pode descobrir e assinar produtos do console do License Manager.

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.

2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Escolha o nome de um produto ou escolha o botão Inscrever-se no AWS Marketplace para exibir os detalhes da assinatura.
4. Para cada um dos produtos listados do Marketplace, selecione Exibir opções de assinatura. Revise os termos e escolha Inscrever-se para continuar.

Se você aceitar os termos, a assinatura do produto precisará ser processada. A assinatura ficará com uma mensagem em andamento até ser concluída. Você poderá repetir essas etapas para todos os outros produtos configurados necessários. Depois que todos os produtos necessários tiverem uma assinatura ativa, você poderá continuar registrando seu Active Directory no produto.

> **Note**
>
> Sua fatura estimada de cobranças sobre o número de usuários e custos relacionados leva 48 horas para aparecer em períodos de cobrança que não foram encerrados (marcados como status de cobrança pendente) em. AWS Billing Para obter mais informações, consulte Como visualizar as cobranças mensais no Guia do usuário do AWS Billing .

Etapa 2: Registrar seu Active Directory no License Manager

O License Manager exige que os usuários da assinatura sejam definidos no Active Directory para associá-los às assinaturas baseadas no usuário. Isso pode ser um Active Directory AWS Managed Microsoft AD ou um Active Directory autogerenciado, dependendo de suas assinaturas.

- Se você assinar somente produtos autônomos do Microsoft Office ou do Visual Studio, deverá configurar um. AWS Managed Microsoft AD
- Se você assinar o Win Remote Desktop Services SAL, poderá usar um Active Directory AWS Managed Microsoft AD ou um autogerenciado Active Directory.

Para usar o Microsoft Office com assinaturas baseadas em usuário, você deve conceder permissão ao License Manager para atualizar sua configuração de VPC. Quando você configura sua VPC, o License Manager cria VPC endpoints em seu nome. Esses endpoints são necessários para que seus atributos se conectem aos servidores de ativação e permaneçam em conformidade.

Você deve configurar o encaminhamento de DNS para qualquer item adicional VPCs que você registre para assinaturas baseadas em usuário. Se você tiver várias assinaturas baseadas em

usuário Regiões da AWS, cada região deverá ter seu próprio Active Directory com encaminhamento de DNS configurado.

> **Important**
>
> Você deve permitir que o License Manager crie o perfil vinculado ao serviço necessária antes de continuar. Para obter mais informações, consulte o Pré-requisitos para criar assinaturas baseadas no usuário no License Manager.

As etapas de registro são diferentes no console, dependendo dos produtos que você assinou. Se você se inscreveu`Win Remote Desktop Services SAL`, selecione a guia Microsoft RDS SAL. Se você assinar o Microsoft Office ou o Visual Studio e NÃO assinar o RDS SAL, selecione a guia Assinaturas MSO autônomas.

> **Important**
>
> Se você já registrou um tipo de produto do Microsoft Office (Office LTSC Professional Plus ou Office LTSC Standard) com um Active Directory em uma VPC e está registrando o outro tipo de produto do Microsoft Office com o mesmo Active Directory na mesma VPC, você deve usar as mesmas sub-redes e o mesmo grupo de segurança da configuração existente do provedor de identidade.

Microsoft RDS SAL

Registre-se AWS Managed Microsoft AD

Para se registrar AWS Managed Microsoft AD como seu Active Directory para assinaturas baseadas em usuário, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Navegue até Assinaturas baseadas no usuário em Configurações no painel de navegação esquerdo.
3. Na guia Serviços de Área de Trabalho Remota (RDS) na página Assinaturas baseadas no usuário, escolha Registrar o Active Directory.
4. Selecione a opção AWS Managed Active Directory para inserir detalhes.

5. Selecione seu diretório gerenciado na lista do AWS Active Directory ou crie um novo diretório gerenciado e, em seguida, volte e selecione-o.
6. Escolha Registrar para registrar seu Active Directory AWS gerenciado.

Registre o Active Directory autogerenciado

Para registrar um Active Directory autogerenciado para assinaturas baseadas em usuário, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Navegue até Assinaturas baseadas no usuário em Configurações no painel de navegação esquerdo.
3. Na guia Serviços de Área de Trabalho Remota (RDS) na página Assinaturas baseadas no usuário, escolha Registrar o Active Directory.
4. Selecione a opção Active Directory autogerenciado para inserir detalhes.
5. Insira o domínio do Active Directory.
6. Selecione a versão dos endereços IP do Active Directory e, em seguida, insira os endereços IP primário e secundário do seu diretório.
7. Na seção Rede, selecione a VPC e as duas sub-redes em que seu Active Directory reside.
8. Selecione o segredo de credenciais administrativas que você criou como parte dos pré-requisitos para sua assinatura do Microsoft RDS.

Stand-alone MSO subscriptions

Registre-se AWS Managed Microsoft AD

Para se registrar AWS Managed Microsoft AD como seu Active Directory para assinaturas do Microsoft Office e do Visual Studio baseadas em usuário, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Navegue até Assinaturas baseadas no usuário em Configurações no painel de navegação esquerdo.
3. Na página Assinaturas baseadas no usuário, selecione a guia do produto de assinatura do Microsoft Office ou do Visual Studio que você deseja registrar e escolha Registrar o Active Directory.

4. Selecione seu diretório gerenciado na lista do AWS Active Directory ou crie um novo diretório gerenciado e, em seguida, volte e selecione-o.
5. Escolha Registrar para registrar seu Active Directory AWS gerenciado.

Quando você registra seu Active Directory, o License Manager cria duas interfaces de rede para que o serviço possa se comunicar com seu diretório. A interface de rede terá uma descrição semelhante à interface de rede AWS criada para LicenseManager *<directory_id>*.

Registro do Active Directory a partir do AWS CLI

Você pode registrar seu Active Directory como provedor de identidade para assinaturas baseadas em usuário com a operação. RegisterIdentityProvider

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product-name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}"
```

Configure o Active Directory e sua VPC para assinaturas baseadas em usuário ()AWS CLI

Você pode registrar seu Active Directory como provedor de identidade e configurar sua VPC para assinaturas baseadas em usuário com a operação. RegisterIdentityProvider

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product_name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}" --settings
 "Subnets=[subnet-1234567890abcdef0,subnet-021345abcdef6789],SecurityGroupId=sg-1234567890abcde
```

Para obter mais informações sobre produtos de software disponíveis, consulte Produtos de software compatíveis para assinaturas baseadas em usuário no License Manager.

> **Note**
>
> Registrar o mesmo Active Directory para o mesmo produto mais de uma vez na mesma região pode resultar em cobranças de assinatura de usuário duplicadas.

Etapa 3: Configurar o servidor de licenças RDS

O servidor de licenças do Microsoft Remote Desktop Services (RDS) emite licenças de acesso de assinante (SALs) aos usuários do Active Directory quando eles acessam instâncias do EC2 que fornecem produtos Microsoft por assinatura com base no usuário. Depois de concluir as etapas 1 e 2, você pode configurar seu servidor de licenças da seguinte maneira.

Certifique-se de ter concluído o formulário User-based pré-requisitos de assinatura RDS antes de começar. Esse processo pressupõe que você já tenha configurado o Active Directory.

Configurar o servidor de licenças RDS para assinaturas baseadas no usuário (console)

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Navegue até a página Assinaturas baseadas no usuário, em Configurações no painel de navegação esquerdo.
3. Na guia Serviços de Área de Trabalho Remota (RDS), você deve ver um ou mais Active Directories na lista. Pode ser exibido um aviso informando que você precisa configurar o RDS para o Active Directory.
4. No prompt ou no menu Ações, escolha Configurar servidor de licenças do RDS.
5. Na caixa de diálogo Configurar servidor de licenças do RDS, você pode definir as seguintes configurações:

   Active Directory

   Esta seção tem detalhes importantes do diretório conectado ao servidor de licenças do RDS que você configura.

   Secret

   Você deve escolher um segredo existente ou criar um novo para as credenciais usadas para tarefas de administração de usuários no servidor de licenças. A primeira parte do nome secreto deve seguir o padrão descrito na seção secreta de credenciais administrativas doUser-based pré-requisitos de assinatura.

   Tags

   Opcionalmente, você pode inserir tags para o recurso do seu servidor de licenças.
6. Escolha Configurar para salvar suas configurações.

Etapa 4: iniciar uma instância para fornecer assinaturas baseadas no usuário

Depois de assinar um produto, você deve iniciar instâncias para que seus usuários se conectem a partir da AWS Marketplace AMI que inclui o produto. Depois de iniciar uma instância, AWS Systems Manager tente unir a instância ao domínio do Active Directory e realizar configurações e fortalecimento adicionais no recurso. As configurações para tornar a instância pronta para uso podem levar cerca de 20 minutos para serem concluídas. Você pode confirmar se o atributo está pronto para uso na página Associação de usuários do console do License Manager verificando o Status de integridade Active para a instância.

Para iniciar uma instância com assinaturas baseadas no usuário, consulte. Execute uma instância a partir de uma licença incluída (AMI)

Etapa 5: associar usuários a uma instância de assinatura baseada em usuário

Depois de assinar a AWS Marketplace AMI do produto necessário, você pode inscrever usuários em um produto e associá-los a uma instância que fornece o produto. Você pode inscrever usuários em produtos e associá-los a uma instância em uma única etapa ou separadamente. Quando você inscreve um usuário, o diretório é verificado para garantir que a identidade do usuário esteja presente. Uma assinatura é criada para cada usuário que você assina no produto.

Cada usuário deve ter uma assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota do Windows Server (RDS SAL) e do produto que usará.

Quando sua conta se inscreve no RDS SAL, conforme detalhado emEtapa 1: assinar um produto, o License Manager inscreve automaticamente os usuários em seu Active Directory no RDS SAL quando eles assinam um produto de assinatura baseado em usuário.

> **Note**
>
> Se um usuário que nunca se inscreveu fizer login em uma instância associada ao RDS SAL, o License Manager o inscreverá automaticamente e iniciará o faturamento do Microsoft RDS. O faturamento continua até que a assinatura seja cancelada e o token de licença emitido pelo servidor de licenças RDS SAL expire.
> Da mesma forma, se um usuário inscrito anteriormente cancelar a assinatura, mas continuar fazendo login após a expiração do token de licença RDS SAL, ele será automaticamente renovado e o faturamento continuará até que a assinatura seja cancelada novamente e seu token expire.

Para obter mais informações sobre cobranças e cobranças de assinatura, consulteCobranças de assinatura no License Manager.

A página Produtos no License Manager exibe assinaturas ativas listando seu status de assinatura do Marketplace como Ativo. Na página de detalhes do produto, o License Manager exibe assinaturas de usuários ativos com um status de Subscribed.

> **Important**
>
> Se o Active Directory não estiver configurado com o produto, uma barra de notificação aparecerá na parte superior do console recomendando que você ajuste as configurações do diretório. Na barra de notificação, escolha Abrir configurações para acessar a página Configurações no License Manager e editar o diretório.
> Cada usuário deve ter uma assinatura do RDS SAL e do produto que usará. A assinatura de usuários em um produto no qual o status da assinatura do Marketplace é Inativo falhará.

Inscrever usuários em um produto e associá-los a uma instância

Ao selecionar uma instância à qual associar usuários, você pode, opcionalmente, inscrevê-los nos produtos que a instância fornece, caso ainda não estejam inscritos. Use um dos métodos a seguir para inscrever e associar usuários.

Console

Para associar usuários a uma instância, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Selecione a instância à qual você deseja associar os usuários e, em seguida, escolha uma das seguintes opções:

   Associar usuários

   Especifique até 5 nomes de usuário que existem em seu diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Associar. Se você usar esse método, os usuários já devem estar inscritos nos produtos que a instância fornece.

Inscrever-se e associar usuários

Especifique até 5 nomes de usuário que existem em seu diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Inscrever-se e associar.

(Opcional) Revise as associações de usuários

Na página Associação de usuários, os usuários selecionados são exibidos em Usuários com um status de associação de Associado.

(Opcional) Revise os usuários inscritos

Na página Produtos, escolha o nome do produto. Os usuários inscritos são exibidos em Usuários com status de Inscrito.

AWS CLI

É possível associar usuários a uma instância executada para fornecer a assinatura baseada no usuário com a operação AssociateUser.

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}"
```

Para associar usuários autogerenciados do Active Directory a uma instância (AWS CLI)

É possível associar usuários a uma instância executada a partir do Active Directory autogerenciado para fornecer a assinatura baseada no usuário com a operação AssociateUser.

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}" --domain <self-managed-domain-name>
```

Para obter mais informações sobre produtos de software disponíveis, consulte Produtos de software compatíveis para assinaturas baseadas em usuário no License Manager.

Inscrever usuário em um produto

Você pode inscrever usuários em um produto usando um dos métodos a seguir.

Console

Inscrever usuários em um produto (Console)

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Selecione um produto para inscrever usuários no qual o status da assinatura do Marketplace seja Ativo.
4. Se o produto for Microsoft RDS, selecione o Active Directory registrado que contém os usuários a serem assinados.
5. Escolha Inscrever usuário para continuar.
6. Especifique até 20 nomes de usuário que existem em seu diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Inscrever-se.

   Os usuários que têm uma assinatura são exibidos em Usuários com status de Assinado.

AWS CLI

Inscrever usuários em um produto (AWS CLI)

Você pode inscrever usuários em um produto registrado com seu provedor de identidade usando a operação StartProductSubscription.

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 ""ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}"
```

Inscrever usuários em um produto com um Active Directory autogerenciado ()AWS CLI

Você pode inscrever usuários do seu Active Directory autogerenciado em um produto registrado em seu AWS Managed Microsoft AD diretório usando a StartProductSubscriptionoperação.

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 'ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}' --
domain <self-managed-domain-name>
```

Para obter mais informações sobre produtos de software disponíveis, consulte Produtos de software compatíveis para assinaturas baseadas em usuário no License Manager.

Os usuários que estiverem inscritos serão exibidos em Usuários com status de Inscrito.

Configurar o GPO do Active Directory para sessões de usuário remoto mais ativas

Por padrão, o Microsoft RDS permite no máximo duas sessões de usuário ao mesmo tempo em uma instância EC2 do Windows que fornece produtos de assinatura baseados no usuário. Depois de configurar seus endpoints do Servidor de Licenças do RDS, você pode configurar o Microsoft RDS para permitir mais de duas sessões de usuário ao mesmo tempo com um Objeto de Política de Grupo (GPO) do Active Directory, da seguinte maneira.

Pré-requisito

Você deve ter criado um servidor de licenças em seu ambiente. Para criar um servidor de licenças, consulteEtapa 3: Configurar o servidor de licenças RDS.

1. A ferramenta que você usa para configurar seu GPO depende de onde você o executa, da seguinte forma:

   Configuração central do seu controlador de domínio

   Faça login no controlador de domínio do Active Directory como administrador e abra o Console de Gerenciamento de Política de Grupo do Windows.

   Configurar a política de grupo no host da sessão

   Faça login no seu Servidor de Licenças como administrador e abra o Editor de Política de Grupo Local.
2. No console de gerenciamento ou no editor de políticas, edite a política de grupo para especificar os hosts de sessão que se conectam por meio do Microsoft RDS. Você pode encontrar o endpoint do seu RDS License Server na página de detalhes do produto License Manager ou com o comando list-license-server-endpoints no. AWS CLI
3. Defina o modo de licenciamento do Host de Sessão de Área de Trabalho Remota para `Per User` e salve.

Para obter mais informações sobre como configurar seu RDS License Server para o License Manager, consulte the section called “Etapa 3: Configurar o RDS” o tópico Get Started. Para obter

mais informações sobre a configuração de hosts de sessão do Microsoft RDS, consulte Licenciar hosts de sessão de área de trabalho remota.

Comece com Cross-Account AWS License Manager usando Compartilhado AWS Managed Microsoft AD

AWS O License Manager oferece suporte à funcionalidade de várias contas usando um compartilhamento AWS Managed Microsoft AD, permitindo que as organizações gerenciem centralmente as assinaturas de usuários a partir de uma conta do proprietário do diretório enquanto implantam instâncias em várias contas.

Terminologia

- Conta do proprietário do diretório - conta de administrador de licenças em que o AD gerenciado existe e que também é responsável pelo gerenciamento de assinaturas.
- Conta de consumidor do diretório — AWS contas nas quais você deseja iniciar instâncias de assinaturas de usuários usando o AD compartilhado.

Pré-requisitos

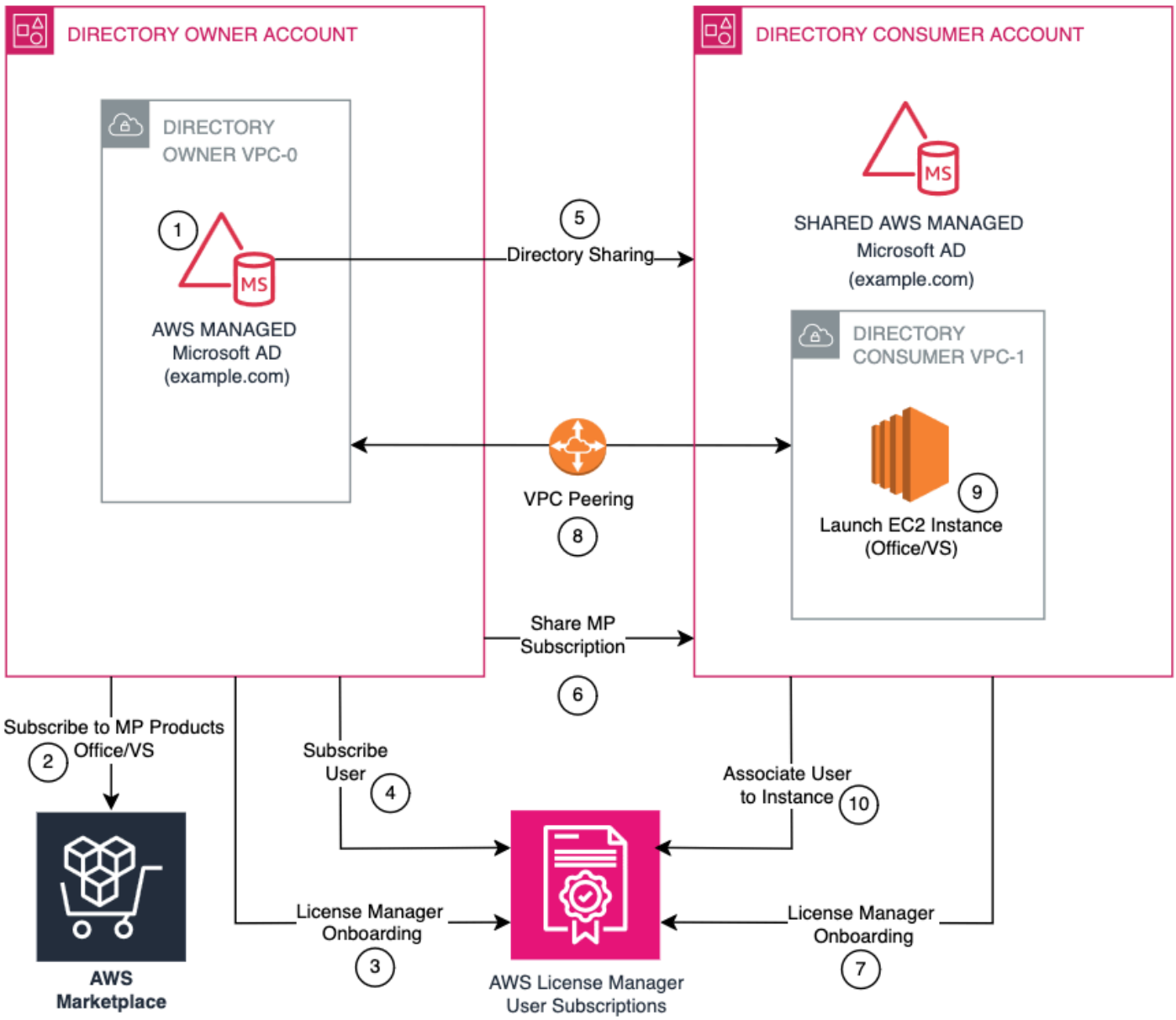
Antes de começar, verifique se você tem:

- Uma AWS Managed Microsoft AD na conta do proprietário do diretório - configure na conta de account/license administrador do proprietário do diretório a partir da qual você deseja controlar as assinaturas.
- Conectividade de rede entre a conta do proprietário do diretório e todas as contas de consumidor do diretório.
- Permissões do IAM necessárias — consulte as funções do IAM por User-based assinatura.
- Assinaturas dos produtos do License Manager necessários AWS Marketplace na conta do proprietário do diretório:
  - Visual Studio Profissional 2022
  - Visual Studio Enterprise 2022
  - Escritório LTSC Professional Plus
  - Padrão LTSC de escritório

Limitações

- O gerenciamento de assinaturas de usuários é restrito à conta do proprietário do diretório.
- Cross-region o compartilhamento não é suportado.
- Faturamento consolidado por meio da conta do proprietário do diretório - todos os custos da assinatura são cobrados na conta do proprietário do diretório, embora as assinaturas possam existir em várias contas.
- É necessária conectividade de rede entre contas.

Arquitetura de rede



Como configurar a funcionalidade do License Manager entre contas

Para configurar a funcionalidade do License Manager entre contas:

1. Configure a conta de account/license administrador do proprietário do diretório.
2. Configure contas de consumidores do diretório.
3. Estabeleça conectividade de rede.
4. Implante instâncias e gerencie associações de usuários.

Etapa 1: configurar a conta de Owner/license administrador do Directory

Crie e compartilhe AWS Managed Microsoft AD

1. Crie um AWS Managed Microsoft AD em sua VPC se ele não existir.
2. Compartilhe o diretório com contas de consumidores do diretório, conforme descrito em Compartilhando seu diretório.
3. Certifique-se de que o diretório esteja configurado corretamente com os usuários e grupos necessários.

Inscrever-se em produtos

1. Navegue até AWS Marketplace.
2. Localize e assine seus produtos necessários, Visual Studio ou Office e RDS SAL.
3. Compartilhe a assinatura do Visual Studio ou do Office com as contas de consumidores do diretório usando o License Manager Create Grants. Como alternativa, você pode assinar AWS Marketplace produtos nessas contas, pois isso não afeta o faturamento. Consulte Licenças concedidas.
4. Verifique se o status da assinatura está ativo.

Registre-se no License Manager

1. Acesse o console do gerenciador de licença da .
2. Navegue até as User-based configurações de assinaturas.
3. Selecione Registrar provedor de identidade.
4. Escolha o seu AWS Managed Microsoft AD.
5. Conclua o processo de registro.

Etapa 2: configurar contas de consumidores do diretório - contas com AD compartilhado

Aceitar diretório compartilhado

1. Abra o console AWS do Directory Service.
2. Navegue até Diretórios compartilhados.
3. Localize e aceite o convite do diretório compartilhado.

4. Anote o novo ID do diretório atribuído à sua conta.

Aceitar assinatura MP

No License Manager Grants, aceite a concessão de AWS Marketplace produtos. Como alternativa, assine os AWS Marketplace produtos. Saiba mais na CreateGrant API).

Registre-se no License Manager

1. Acesse o console do gerenciador de licença da .
2. Navegue até User-based assinaturas e escolha o produto.
3. Registre-se usando o ID do diretório compartilhado e o produto.
4. Verifique o status de registro.

Etapa 3: Estabelecer conectividade de rede entre VPCs

Para unir por domínio suas instâncias do Amazon Amazon EC2 ao seu diretório, você precisa estabelecer conectividade de rede entre as VPCs. Há várias opções para estabelecer conectividade de rede entre duas VPCs. Esta seção mostra como usar o peering do Amazon VPC.

Configurar o emparelhamento da VPC

1. Crie uma conexão de emparelhamento de VPC entre o proprietário VPC-0 e o consumidor do diretório e, em seguida VPC-1, crie outra conexão entre o proprietário VPC-0 e o consumidor do diretório. VPC-2
2. Ative o roteamento de tráfego entre as VPCs emparelhadas adicionando uma rota à sua tabela de rotas da VPC que aponta para a conexão de emparelhamento da VPC para rotear o tráfego para a outra VPC na conexão de emparelhamento.
3. Configure cada uma das tabelas de rotas VPC do consumidor do diretório adicionando a conexão de emparelhamento com o proprietário do diretório. VPC-0 Se quiser, você também pode criar e conectar um Internet Gateway às VPCs consumidoras do seu diretório. Isso permite que as instâncias nas VPCs consumidoras do diretório se comuniquem com o agente do Amazon EC2 Systems Manager que realiza a união do domínio.

Configurar grupos de segurança

Configure o grupo de segurança das VPCs consumidoras de seu diretório para ativar o tráfego de saída adicionando AWS Managed Microsoft AD os protocolos e as portas à tabela de regras de saída. Além disso, configure o grupo de segurança das VPCs dos controladores de domínio de seu diretório para habilitar o tráfego de entrada adicionando AWS Managed Microsoft AD os protocolos e as portas à tabela de regras de entrada, para permitir o tráfego de contas de consumidores do diretório.

Requisitos para grupos de segurança

VPCs de contas de consumidores:

- Habilitar tráfego de saída para a VPC do proprietário do diretório
- Permitir comunicação nas portas AD necessárias

Proprietário do diretório VPC:

- Configurar o tráfego de entrada de VPCs de consumidores
- Adicione AWS Managed Microsoft AD os protocolos e portas necessários, incluindo:
  - TCP 53 (DNS)
  - UDP 35 (DNS)
  - TCP 88 (Kerberos)
  - UDP 88 (Kerberos)
  - TCP 135 (RPC)
  - TCP 389 (LDAP)
  - UDP 389 (LDAP)
  - TCP 445 (SMB)
  - TCP 464 (senha Kerberos)
  - UDP 464 (senha Kerberos)
  - TCP 636 (LDAPS)
  - TCP 9389 (Serviços Web do Active Directory)
  - TCP 3268-3269 (Catálogo global)
  - TCP 1024-65535 (RPC dinâmico)

A porta 9389 é necessária para os Serviços Web do Active Directory (ADWS), que é usada pelo PowerShell módulo Active Directory e outras ferramentas de gerenciamento para se comunicar com controladores de domínio.

Etapa 4: implantar instâncias e gerenciar associações de usuários

Inscrever usuários (somente conta do proprietário do diretório)

1. Acesse o console do gerenciador de licença da .
2. Navegue até User-based assinaturas.
3. Selecione Assinar usuários
4. Insira identificadores AWS Managed Microsoft AD de usuário
5. Escolha o produto e confirme a assinatura.

Iniciar instâncias

Execute essa etapa em qualquer conta.

1. Navegue até o console do Amazon EC2.
2. Escolha Executar instância.
3. Selecione a AMI do License Manager apropriada.
4. Defina as configurações de rede.
5. Análise e lançamento.

Associar usuários a instâncias

Execute essa etapa em qualquer conta em que a instância exista.

1. Abra o console do License Manager.
2. Navegue até Associações de usuários.
3. Selecione a instância de destino.
4. Escolha Associar usuários.
5. Insira os AWS Managed Microsoft AD nomes de usuário.
6. Confirme a associação.

Solução de problemas

Problemas e soluções comuns:

Falhas na junção de domínio

1. Verifique a conectividade de rede entre as contas.
2. Verifique as configurações do grupo de segurança.
3. Confirme se a resolução do DNS está funcionando.
4. Valide as entradas da tabela de rotas.

Problemas com a assinatura do usuário

1. Confirme se o usuário existe em AWS Managed Microsoft AD.
2. Verifique o status da assinatura na conta do proprietário do diretório.
3. Verifique a conectividade da rede.
4. Revise os registros de erros.

Problemas de conectividade de rede

1. Teste o status da conexão de emparelhamento de VPC.
2. Verifique as configurações da tabela de rotas.
3. Confira as regras do grupo de segurança.
4. Confirme a resolução do DNS.

Problemas de resolução de DNS

1. Verifique os conjuntos de opções DHCP.
2. Verifique as configurações do servidor DNS.
3. Teste a resolução de nomes de instâncias de consumidores.

Recursos adicionais do

- AWS Guia do usuário do License Manager
- AWS Documentação do Directory Service

- Compartilhando seu diretório
- Como unir um domínio a instâncias do Amazon EC2 para direcionar AWS Managed Microsoft AD várias contas e VPCs
- Licenças concedidas

Execute uma instância a partir de uma licença incluída (AMI)

Depois de assinar um produto, você deve iniciar instâncias para que seus usuários se conectem a partir da AWS Marketplace AMI que inclui o produto. Depois de iniciar uma instância, AWS Systems Manager tente unir a instância ao domínio do Active Directory e realizar configurações e fortalecimento adicionais no recurso. As configurações para tornar a instância pronta para uso podem levar cerca de 20 minutos para serem concluídas. Você pode confirmar se o atributo está pronto para uso na página Associação de usuários do console do License Manager verificando o Status de integridade Active para a instância.

> **Important**
>
> As instâncias que você executa devem atender aos pré-requisitos exigidos para estarem em conformidade. Os recursos que não conseguem concluir a configuração inicial são encerrados. Para obter mais informações, consulte Pré-requisitos para criar assinaturas baseadas no usuário no License Manager e Solucionar problemas de assinaturas baseadas em usuário no License Manager.

Execute uma instância com assinaturas baseadas no usuário

1. Acesse o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Em Imagens, escolha Catálogo AMI.
3. Escolha AWS Marketplace AMIs.
4. Insira o nome do produto na caixa de pesquisa e pressione enter. Por exemplo, você pode pesquisar por **`Visual Studio`**.
5. Em Publicador, selecione Amazon Web Services.
6. Escolha Selecionar para o produto que deseja executar uma instância para fornecer assinaturas baseadas no usuário.
7. Escolha Continuar para prosseguir.

8. Escolha Executar instância com AMI.
9. Execute o assistente e garanta que:
    a. Escolherá um tipo de instância baseada em Nitro que não seja baseada em Graviton.
    b. Escolherá uma VPC e uma sub-rede a partir das quais a instância possa se conectar ao diretório do AWS Managed Microsoft AD .
    c. Escolha um grupo de segurança que permita a conectividade da sua instância com o Active Directory.
    d. Expanda Detalhes avançados e escolha um perfil do IAM que permita a funcionalidade do Systems Manager para sua instância.
10. Escolha Iniciar instância.

Ao executar instâncias da AWS Marketplace AMI, você deve inscrever usuários no produto e associá-los às instâncias, que fornecem o produto para que eles possam usá-lo.

Execute uma instância a partir de uma versão específica do sistema operacional (AMI)

Quando você executa uma instância de uma AMI que oferece suporte ao Office LTSC Professional Plus, Office LTSC Standard ou Microsoft Visual Studio, a execução usa como padrão a versão mais recente da AMI do sistema operacional Windows (por exemplo, Windows Server 2025). Para iniciar com uma versão específica da AMI do sistema operacional, siga estas etapas.

1. Abra o AWS Marketplace console em https://console.aws.amazon.com/marketplace.
2. No painel de navegação, escolha Gerenciar assinaturas.
3. Para otimizar os resultados da assinatura, você pode pesquisar todo ou parte do nome da assinatura. Por exemplo, `Office LTSC Professional Plus`, `Office LTSC Standard` ou `Visual Studio Enterprise`.
4. Selecione Iniciar nova instância no painel de assinatura. Isso abre uma página de configuração de execução.
5. Para iniciar uma instância a partir de uma AMI baseada em uma versão anterior da plataforma do sistema operacional Windows, selecione o link completo AWS Marketplace do site, localizado abaixo da versão do software. Isso leva você a uma página de configuração na qual você pode selecionar em uma lista de versões.
6. A lista mostra as versões mais recentes da AMI para as plataformas de sistema operacional Windows compatíveis. Selecione a versão do sistema operacional Windows a partir da qual você deseja iniciar.

Execute uma instância com os produtos Microsoft Office e Microsoft Visual Studio

Você pode iniciar uma instância do EC2 que tenha os produtos Microsoft Office e Microsoft Visual Studio pré-instalados usando uma única AMI criando um pipeline do EC2 Image Builder por meio do License Manager. O pipeline cria uma AMI dourada que agrupa seus produtos selecionados — por exemplo, Visual Studio Professional 2022 e Office LTSC Professional Plus 2024 — em uma única AMI. Em seguida, você pode executar instâncias dessa AMI com todos os produtos prontos para uso.

Pré-requisitos

Antes de criar o pipeline do EC2 Image Builder por meio do License Manager, certifique-se do seguinte:

- Você tem assinaturas ativas do AWS Marketplace para pelo menos dois produtos de assinatura baseados no usuário (por exemplo, uma assinatura do Visual Studio Enterprise e uma assinatura do Office LTSC Professional).
- Você tem uma configuração de infraestrutura do EC2 Image Builder em sua conta. Isso define a VPC, a sub-rede, os grupos de segurança e o perfil da instância do IAM que o Image Builder usa ao criar a imagem. Se você não tiver um, crie-o no console do EC2 Image Builder.

Etapa 1: criar um pipeline de criação de imagens EC2 com vários produtos

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, em User-basedassinaturas, escolha Produtos e funis.
3. Escolha a guia Pipelines do EC2 Image Builder.
4. Selecione Criar pipeline.
5. Para a versão Windows, selecione a versão necessária do Windows Server.
6. Para Produtos, selecione dois ou mais produtos licenciados para incluir. Somente os produtos dos quais você está inscrito no AWS Marketplace e compatíveis com a versão selecionada do Windows são exibidos.
7. Para a configuração da infraestrutura do EC2 Image Builder, selecione uma configuração de infraestrutura existente em sua conta.
8. Selecione Criar pipeline.

Após a criação, o License Manager cria a receita e o pipeline de imagem subjacentes no EC2 Image Builder. Você pode executar o pipeline imediatamente a partir do console do EC2 Image Builder.

> **Note**
>
> O License Manager criará somente o pipeline e a receita correspondente necessária para criar a AMI de vários produtos. Você pode gerenciar e atualizar o pipeline por meio do console do EC2 Image Builder.

Etapa 2: executar o pipeline para produzir uma AMI

1. Na guia Pipelines do EC2 Image Builder, selecione seu pipeline e escolha Exibir no Image Builder.
2. No console do EC2 Image Builder, escolha Run pipeline para iniciar uma compilação.
3. Aguarde a conclusão da compilação.

Etapa 3: executar uma instância a partir da AMI de vários produtos

Depois que a construção do pipeline for concluída, você poderá executar uma instância a partir da AMI de saída usando um dos métodos a seguir.

Opção A: iniciar a partir do console do EC2 Image Builder

1. No console do EC2 Image Builder, abra o pipeline que concluiu a compilação.
2. Em Imagens de saída, encontre a AMI produzida pela versão mais recente.
3. Escolha o link da AMI para abri-lo no console do EC2 e, em seguida, escolha Launch instance from AMI.
4. Conclua o assistente de inicialização e, ao mesmo tempo, garanta que você:
    a. Escolha um tipo de Nitro-based instância que não sejaGraviton-based.
    b. Escolha uma VPC e uma sub-rede a partir das quais sua instância possa se conectar ao seu diretório. AWS Managed Microsoft AD
    c. Escolha um grupo de segurança que permita a conectividade da sua instância com o Active Directory.
    d. Expanda Detalhes avançados e escolha um perfil do IAM que permita a funcionalidade do Systems Manager para sua instância.

5. Escolha Iniciar instância.

Opção B: iniciar a partir do console EC2

1. Acesse o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Em Imagens, escolha AMIs.
3. Encontre a AMI produzida pelo seu pipeline. Pipeline-produced As AMIs têm nomes prefixados com. `license-manager-created-`
4. Selecione a AMI e escolha Launch instance from AMI.
5. Conclua o assistente de inicialização e, ao mesmo tempo, garanta que você:
   a. Escolha um tipo de Nitro-based instância que não sejaGraviton-based.
   b. Escolha uma VPC e uma sub-rede a partir das quais sua instância possa se conectar ao seu diretório. AWS Managed Microsoft AD
   c. Escolha um grupo de segurança que permita a conectividade da sua instância com o Active Directory.
   d. Expanda Detalhes avançados e escolha um perfil do IAM que permita a funcionalidade do Systems Manager para sua instância.
6. Escolha Iniciar instância.

A instância é iniciada com todos os produtos licenciados selecionados pré-instalados e pré-licenciados. Depois que a instância estiver ativa no console do License Manager, inscreva os usuários nos produtos correspondentes e associe-os à instância para que possam usá-la.

Conecte-se a uma instância de assinatura baseada em usuário com o RDP

Depois de associar os usuários à instância que fornece o produto, eles podem se conectar à instância se o status de integridade da instância for Ativo. Os usuários precisarão se conectar com suas credenciais de usuário do domínio para usar o produto com a identidade associada.

> **Important**
>
> O processo de criar a instância do EC2 e prepará-la para os usuários pode levar cerca de 20 minutos. O status de associação da instância deve ser Ativo para acessá-la e usar o produto.

Para se conectar a uma instância de assinatura baseada no usuário

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação esquerdo, em User-basedassinaturas, escolha Associação de usuário.
3. Na página Associação de usuário, confirme se o status de integridade da instância está Ativo.
4. Anote o ID da instância, pois você precisará dele para coletar os detalhes da conexão.
5. Siga as etapas listadas em Conectar sua instância do Windows usando RDP e, ao mesmo tempo, certifique-se de especificar o nome de usuário totalmente qualificado do usuário associado.

Modifique as configurações de firewall para sua assinatura do Microsoft Office

Um firewall protege seus recursos de rede contra tráfego de entrada ou saída não autorizado. As regras que você define para seu grupo de segurança atuam como firewall para os recursos de VPC que trabalham juntos para fornecer assinaturas baseadas no usuário do Microsoft Office em instâncias do Windows do EC2.

Você pode usar as etapas a seguir para editar as sub-redes e o grupo de segurança. O License Manager usa suas configurações para provisionar endpoints para o Microsoft Office com AWS PrivateLink. Para obter mais informações sobre VPC endpoints, consulte O que é? AWS PrivateLink na documentação da Amazon Virtual Private Cloud.

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Navegue até a página de User-based assinaturas, em Configurações no painel de navegação esquerdo.
3. Para editar as configurações do firewall, selecione a guia do produto de assinatura do Microsoft Office e escolha Editar na parte superior da seção Firewall. Isso abre a caixa de diálogo Editar firewall.
4. Depois de alterar suas configurações, escolha Salvar para atualizar ou Cancelar para manter as configurações atuais.

Pode levar alguns minutos para que o License Manager conclua as alterações nessas configurações.

Gerencie usuários de assinatura para assinaturas baseadas em usuários do License Manager

Para garantir a precisão da cobrança e dos relatórios das assinaturas de produtos do Microsoft Office e do Visual Studio no License Manager e para evitar o acesso não autorizado aos recursos da assinatura, você pode gerenciar o acesso do usuário da seguinte maneira.

Desassociar usuários de uma instância

Desassocie um usuário de uma instância que hospeda uma assinatura de produto Microsoft Office ou Visual Studio baseada no usuário do License Manager para remover o acesso ao recurso.

Cancelar a inscrição de usuários

Cancele a assinatura de usuários de assinaturas de produtos Microsoft Office ou Visual Studio baseadas em usuários AWS License Manager para parar de incorrer em cobranças de assinatura para essas pessoas.

> **Note**
>
> A exclusão de um usuário do Active Directory não alterará as associações de usuários nem as assinaturas dos produtos Microsoft Office e Visual Studio. Você deve desassociar o usuário no License Manager da página de detalhes do produto de assinatura para remover sua associação com uma instância. Em seguida, você deve cancelar a inscrição do usuário. Este tópico não aborda a administração do Active Directory.

Conteúdo

Desassociar usuários de uma instância que fornece assinaturas baseadas no usuário do License Manager

Para remover o acesso do usuário a uma instância que fornece assinaturas baseadas no usuário do License Manager, você pode desassociar o usuário inscrito dessa instância. Essa alteração não afeta o status da assinatura do usuário. Para cancelar a assinatura de um usuário e interromper as cobranças de assinatura dessa pessoa, consulteCancele a assinatura de usuários de assinaturas de produtos com base no usuário no License Manager.

Desassociar usuários de assinatura de uma instância

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Selecione a instância da qual você quer desassociar os usuários.
4. Selecione os nomes de usuário a serem desassociados e, em seguida, escolha Desassociar usuários.

Cancele a assinatura de usuários de assinaturas de produtos com base no usuário no License Manager

Você deve cancelar a assinatura de um usuário de um produto de assinatura baseado em usuário do Microsoft Office ou do Visual Studio para parar de incorrer em cobranças por ele. O Microsoft RDS é cobrado por usuário, por mês, com base em uma combinação da assinatura do usuário e do token da licença de acesso do cliente (CAL) emitido pelo servidor de licenças quando o usuário se conecta a uma instância que fornece o produto de assinatura. Para obter mais informações, consulte Cobrança do Microsoft RDS no License Manager.

> **Important**
>
> Para produtos de assinatura com base no usuário do Microsoft Office ou do Visual Studio, você deve primeiro desassociar o usuário do Active Directory de todas as instâncias em que ele está atualmente associado antes de poder cancelar a assinatura.

Cancelar a inscrição de usuários de assinaturas de produtos com base no usuário

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Selecione o produto do qual você deseja cancelar a assinatura de usuários.
4. Selecione os nomes de usuário para cancelar a assinatura e, em seguida, escolha Cancelar assinatura de usuários.

Cancelar o registro de um Active Directory nas configurações do License Manager

Você pode cancelar o registro do Active Directory nas configurações do License Manager se não quiser mais usá-lo para assinaturas baseadas em usuário. Cancelar o registro da configuração do diretório nas configurações do License Manager não exclui o diretório. Ao cancelar o registro do diretório nas configurações, você não pode mais associar usuários desse diretório para assinaturas baseadas em usuários no License Manager.

Pré-requisitos

Antes de cancelar o registro do diretório nas configurações do License Manager, você deve executar as seguintes tarefas:

1. Desassociar usuários de uma instânciade cada instância que faz referência ao diretório cujo registro você deseja cancelar.
2. Depois que todos os usuários da assinatura forem desassociados da instância, encerre a instância. Repita até que todas as instâncias que se referem ao Active Directory sejam encerradas.
3. Você também precisa pertencer ao Active Directory. Você cancelará o registro para parar de fazer alterações neles. Cancelar a inscrição de usuários

Cancelar o registro

> **Important**
>
> Se o Active Directory for usado para usuários do Microsoft RDS SAL, você deverá excluir o endpoint do servidor de licenças associado antes de cancelar o registro e excluir o AD.

Cancele o registro do Active Directory nas configurações do License Manager

Depois de concluir todas as tarefas de pré-requisito, abra o console do License Manager em. https://console.aws.amazon.com/license-manager/

1. No painel de navegação à esquerda, escolha Configurações.
2. Na página Configurações, na AWS Managed Microsoft AD seção, escolha Remover.
3. Insira o texto necessário para confirmar que você deseja remover o diretório e escolha Remover.

Depois de escolher Remover, a AWS Managed Microsoft ADseção na página Configurações exibe sua ID de diretório com o status de configuração. Quando o processo de configuração estiver concluído, o diretório será removido da AWS Managed Microsoft ADseção.

Solucionar problemas de assinaturas baseadas em usuário no License Manager

Veja a seguir dicas de solução de problemas para ajudar a resolver problemas que podem ocorrer no AWS License Manager com assinaturas baseadas no usuário.

Sumário

- Solucione problemas de contagem de licenças que não estão aparecendo corretamente
- Solucionar problemas do RDS License Diagnoser
- Solucionar problemas de confiança
- Solucionar problemas de cobrança de assinaturas de usuários
- Solucionar problemas de status de assinatura inativa do Marketplace
- Solucione problemas de limites de usuários por instância
- Solucionar problemas do token CAL não vendido após a migração para o RDS SAL
- A união perfeita de domínios não funciona para instâncias do EC2 com produtos de assinatura de usuário
- O VPC endpoint foi criado em minha conta
- Remova todos os recursos de VPC endpoint criados pelo License Manager
- Alterar um nome de usuário no Managed Active Directory
- Dissociar usuários de uma instância encerrada
- Instale software adicional em instâncias de assinatura de usuários
- Pacotes de idioma japonês em instâncias de assinatura de usuários
- Usuário administrador local em instâncias de assinatura de usuário
- Número de usuários que podem usar RDP para uma instância de assinaturas de usuários
- Usuários em meus produtos autogerenciados do AD para Office e Visual Studio
- Sistemas operacionais Windows compatíveis
- Versões compatíveis do Office e do Visual Studio
- Usando a assinatura de usuário com versões mais antigas do Windows Server
- Usando assinaturas de usuário do License Manager em todas as contas ou regiões
- Dicas para entrar em contato com o AWS Support

Solucione problemas de conformidade de instâncias

As instâncias que fornecem assinaturas baseadas no usuário devem permanecer com status íntegro para estarem em conformidade. As instâncias marcadas como não íntegras não atendem mais aos pré-requisitos exigidos. O License Manager tentará retornar a instância ao status íntegro, mas as instâncias que não conseguirem retornar ao status íntegro serão terminadas.

As instâncias que forem executadas para fornecer assinaturas baseadas no usuário e não conseguirem concluir a configuração inicial serão terminadas. Você deve corrigir o problema de

configuração e executar novas instâncias para fornecer assinaturas baseadas no usuário nesse cenário. Para obter mais informações, consulte o Pré-requisitos para criar assinaturas baseadas no usuário no License Manager.

Solucionar problemas de falha na configuração do produto de assinatura de usuário

A configuração do seu produto pode estar falhando devido a problemas com o acesso externo à rede. Para resolver isso, certifique-se de que o grupo de segurança padrão permita tráfego de saída para os endereços IP da interface de rede de cada controlador de domínio, bem como para o SSM.

- Verifique se as configurações padrão do grupo de segurança facilitam o tráfego de saída para os endereços IP das interfaces de rede do controlador de domínio.
  - O License Manager cria duas interfaces de rede que usam o grupo de segurança padrão da VPC em que a sua AWS Managed Microsoft AD está provisionada. Essas interfaces são usadas para a funcionalidade de serviço necessária com o diretório. Certifique-se de que seu grupo de segurança padrão permita tráfego de saída para o endereço IP da interface de rede de cada controlador de domínio ou para o grupo de segurança usado pelos controladores de domínio. Para obter mais informações, consulte Pré-requisitos para criar assinaturas baseadas no usuário e O que é criado no Guia de Administração. Directory Service
- Configure o acesso de saída à Internet a partir de instâncias que fornecem assinaturas baseadas no usuário ou VPC endpoints.
  - O acesso de saída à Internet das instâncias que fornecem assinaturas baseadas no usuário, ou VPC endpoints, deve ser configurado para que suas instâncias se comuniquem com o SSM. Para obter mais informações, consulte Configurando o Systems Manager para instâncias do EC2 no Guia do AWS Systems Manager usuário.

Quando o processo de provisionamento estiver concluído, será possível associar um grupo de segurança diferente às interfaces criadas pelo License Manager. O grupo de segurança selecionado também deve permitir o tráfego necessário para o IPv4 endereço da interface de rede ou grupo de segurança de cada controlador de domínio. Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon Virtual Private Cloud.

Solucionar problemas de falhas de lançamento de instâncias de assinatura de usuários

As execuções de sua instância podem estar falhando por vários motivos. Aqui estão alguns dos problemas comuns nos quais a inicialização de uma instância pode falhar:

- Certifique-se de que sua instância possa ser descoberta pelo SSM, consulte. the section called “Solucionar problemas de conectividade da instância”
- Certifique-se de que sua instância seja capaz de se juntar ao seu domínio, consultethe section called “Solucionar falhas ao ingressar no domínio”.
- Certifique-se de que a regra de endpoint do resolvedor de saída Route53 esteja definida. Para obter mais informações, consulte a postagem do blog Integrando a resolução de DNS do seu serviço de diretório com os resolvedores do Amazon Route 53.
- Ao iniciar instâncias personalizadas AMIs criadas em cima da assinatura do usuário AMIs, certifique-se de executar o Sysprep e garantir nomes de computador exclusivos ao criar e executar instâncias personalizadas. AMIs

Solucionar problemas de conformidade de licenças

Se você configurou seu Active Directory para fornecer assinaturas baseadas em usuário com o Microsoft Office, você deve garantir que seus recursos possam se conectar aos endpoints de VPC que o License Manager cria. Os endpoints exigem tráfego de entrada na porta TCP 1688 das instâncias que fornecem assinaturas baseadas no usuário.

É possível usar o Reachability Analyzer para ajudar a confirmar se a configuração de rede das instâncias que fornecem assinaturas baseadas no usuário e os endpoints da VPC estão configurados corretamente. É possível especificar como origem uma ID de instância executada em uma sub-rede que fornece assinaturas baseadas no usuário e um endpoint da VPC provisionado para produtos do Microsoft Office como destino. Especifique TCP como protocolo e 1688 como porta de destino para o caminho a ser analisado. Para obter mais informações, consulte Como posso solucionar problemas de conectividade em meus endpoints da VPC de gateway e interface?.

Solucionar problemas de conectividade da instância

Os usuários devem poder usar o RDP para se conectar às instâncias que fornecem assinaturas baseadas no usuário para usar os produtos contidos. Para obter mais informações sobre como solucionar problemas de conectividade de instâncias, consulte Solucionar problemas de conexão com sua instância do Windows no Guia do usuário do Amazon EC2.

Solucionar falhas ao ingressar no domínio

Os usuários devem poder se conectar às instâncias que fornecem aos produtos de assinatura baseados em usuário suas identidades de usuário do Active Directory configurado nas configurações do License Manager. As instâncias que não conseguirem ingressar no domínio serão encerradas.

Para solucionar o problema, talvez seja necessário executar uma instância e ingressar manualmente no domínio para que o atributo não seja encerrado antes de poder investigar. A instância deve receber e executar o comando de execução do Systems Manager com êxito, e a instância também deve ser capaz de ingressar no domínio dentro do sistema operacional. Para obter mais informações, consulte Compreender os status de comando no Guia do usuário do AWS Systems Manager e Como solucionar erros que ocorrem quando computadores baseados no Windows ingressam em um domínio no site da Microsoft.

Se você iniciar instâncias a partir de uma AMI personalizada que usa uma AMI de produto de assinatura baseada em usuário como imagem base, deverá executar as etapas do Sysprep na AMI personalizada para garantir um nome de computador exclusivo na inicialização. Antes de executar o Sysprep com /generalize, verifique se a máquina foi removida do domínio.

Solucionar problemas de conectividade do Systems Manager

As instâncias que fornecem assinaturas baseadas no usuário devem ser gerenciadas AWS Systems Manager ou serão encerradas. Para obter mais informações, consulte Solução de problemas do SSM Agent e Solução de problemas de disponibilidade do nó gerenciado no Guia do usuário do AWS Systems Manager .

Solucionar problemas do comando Run do Systems Manager

O Run Command, um atributo do Systems Manager, é usado com instâncias que fornecem assinaturas baseadas no usuário para ingressar no domínio, fortalecer o sistema operacional e realizar auditorias de acesso ao produto incluído. Para obter mais informações, consulte Entender os status dos comandos no Guia do usuário do AWS Systems Manager .

Solucionar problemas de falhas de licenciamento do Microsoft RDS

Se você tiver problemas com a emissão de CAL (Licença de Acesso para Cliente), verifique se há servidores de licenciamento Microsoft RDS adicionais presentes em seu farm de servidores ou grupo de servidores de terminal. Não recomendamos ter servidores de licenciamento adicionais nesses locais, pois isso pode interferir na emissão de CAL e levar a complicações de licenciamento.

Para resolver esse problema, certifique-se de que somente os servidores Microsoft RDS pretendidos permaneçam em seu farm de servidores e grupo de servidores de terminal.

Ao solucionar problemas de licenciamento, lembre-se de que as conexões que usam o sinalizador /admin ignoram as verificações de licenciamento padrão, pois esse sinalizador é destinado a fins administrativos e não consome uma CAL. Isso pode mascarar problemas de licenciamento

subjacentes. Para diagnosticar problemas de licenciamento, verifique se as conexões de usuário padrão (sem o sinalizador /admin) estão funcionando corretamente para o gerenciamento de licenças.

Solucionar problemas de falhas de ativação do Microsoft Office

Se a ativação do Microsoft Office falhar, verifique se sua instância tem acesso à VPC definida para o License Manager. Qualquer uma das opções a seguir satisfaz esse requisito:

- Sua instância está sendo executada na VPC integrada ao License Manager (por meio do VPC endpoint)
- Sua instância está sendo executada em uma VPC pareada com a VPC integrada do License Manager.

Para resolver esse problema, certifique-se de que sua instância seja movida para a VPC correta ou estabeleça o emparelhamento de VPC com a VPC integrada do License Manager.

Solucionar problemas de incapacidade de excluir o Active Directory

O License Manager é registrado como um aplicativo autorizado no Directory Service durante a configuração, protegendo assim os diretórios ativos da exclusão depois de configurados. Como parte do procedimento padrão, os clientes precisam primeiro remover todas as instâncias, associações de instâncias e assinaturas de usuários. Depois disso, eles podem prosseguir com a remoção do diretório ativo do License Manager e, posteriormente, excluir o próprio diretório.

Solucionar problemas de incapacidade de excluir a função vinculada ao AWSService RoleFor AWSLicense ManagerUserSubscriptionsService serviço (SLR)

O License Manager exige a função vinculada ao serviço AWSService RoleFor AWSLicense ManagerUserSubscriptionsService "" para gerenciar AWS recursos que fornecerão assinaturas baseadas no usuário. Uma função vinculada ao serviço facilita a configuração do License Manager porque você não precisa adicionar manualmente as permissões necessárias. O License Manager define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o License Manager pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter mais informações, consulte the section called “User-based pré-requisitos de assinatura” License Manager — Função de assinatura baseada no usuário e funções vinculadas ao serviço.

Erro de solução de problemas: a assinatura não está presente para o produto RDS SAL

Sua conta deve ter uma assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota do Windows Server (RDS SAL). Todos os usuários associados às instâncias que fornecem produtos de assinatura com base no usuário devem ter uma única assinatura ativa dessa licença, além de todos os outros produtos que quiserem usar. O usuário será inscrito no RDS SAL em seu nome quando assinar um produto de assinatura baseada no usuário.

Mas se a assinatura tiver sido cancelada ou removida devido a outros motivos de conformidade, talvez você precise se inscrever novamente. Se você já estiver inscrito, tente cancelar e reassinar, o que não afetará suas assinaturas de usuário do License Manager.

Solucione problemas de contagem de licenças que não estão aparecendo corretamente

Após a configuração inicial ou as alterações na configuração, pode levar até 24 horas para que o servidor de licenças exiba contagens precisas de licenças para todos os tipos de licenças no Diagnosticador de Licenças.

O que fazer:

- Aguarde até 24 horas após a configuração antes de esperar um relatório preciso da contagem de licenças

Esse atraso é normal e permite que o servidor de licenças tenha tempo suficiente para sincronizar e atualizar adequadamente todas as informações da licença em diferentes tipos de licença. Se você encontrar um erro, consultethe section called “Solucionar problemas do RDS License Diagnoser”.

Solucionar problemas do RDS License Diagnoser

Esses erros geralmente são causados por problemas de credenciais ou de permissão. Para resolver:

1. Verifique as credenciais do usuário: verifique se você está usando a mesma conta de usuário fornecida ao License Manager durante a integração
2. Verifique as credenciais da sessão: se você ver “Credenciais não disponíveis” no servidor na seção de resumo:
   a. Clique no servidor de licenças na seção de resumo que mostra “Credenciais não disponíveis”

b. No menu do lado direito que se abre, adicione as credenciais do usuário que foi integrado ao License Manager

c. Clique em “Atualizar”

Se o problema persistir, siga as etapas adicionais de solução de problemas descritas na documentação da Microsoft: Não é possível conectar-se ao RDS - Sem servidor de licenças

Isso deve resolver a maioria dos problemas relacionados a credenciais e permissões com o Diagnosticador de Licenças.

Solucionar problemas de confiança

Com base em nossa experiência de trabalho com muitos clientes, a grande maioria dos problemas de configuração de confiança são erros de resolução de DNS ou de conectividade de rede. Estas são algumas etapas de solução de problemas para ajudá-lo a resolver problemas comuns:

- Verifique se você permitiu tráfego de rede de saída no AWS Managed Microsoft AD.
- Se o servidor DNS ou a rede do seu domínio local usar um espaço de endereço IP público (não RFC 1918), siga estas etapas:
  - No Directory Service console, vá para a seção de roteamento IP do seu diretório, escolha Ações e, em seguida, escolha Adicionar rota.
  - Insira o bloco de endereços IP do seu servidor DNS ou rede local usando o formato CIDR, por exemplo, 203.0.113.0/24.
  - Essa etapa não é necessária se o servidor DNS e a rede local estiverem usando espaços de endereço IP privados RFC 1918.
- Depois de verificar o grupo de segurança e verificar se alguma rota aplicável é necessária, inicie uma instância do Windows Server e associe-a ao AWS Managed Microsoft AD diretório. Depois que a instância for iniciada:
  - Execute este PowerShell comando para testar a conectividade DNS:

```
Resolve-DnsName -Name 'example.local' -DnsOnly
```

Você também deve examinar as explicações das mensagens no guia de motivos do status de criação de confiança na Directory Service documentação.

Solucionar problemas de cobrança de assinaturas de usuários

AWS cobrará você por meio de uma assinatura mensal, com base no número de usuários associados à licença, incluindo instâncias do Microsoft Office ou do Visual Studio. Essas cobranças por usuário são cobradas por mês civil, e a cobrança começa no momento em que você assina o produto. Se você remover o acesso a um usuário durante o mês existente, você será cobrado pelo usuário pelo restante do mês. Você deixará de incorrer em cobranças para o usuário no mês seguinte.

Além disso:

- O faturamento é baseado em uma base por usuário nas assinaturas do usuário. Somente os usuários inscritos no produto incorrerão em cobranças, nem todos os usuários do Active Directory.
- O faturamento opera em um ciclo mensal, começando no primeiro dia de cada mês civil. As cobranças são cobradas durante todo o mês, independentemente da data específica de ativação da assinatura.
- Você precisa de um RDS SAL para cada usuário que precisa acessar suas Office/VS instâncias.
- Para parar de incorrer em cobranças por assinaturas baseadas no usuário, você deve desassociar o usuário de todas as instâncias às quais ele está associado. A exclusão de um usuário do Active Directory não dissocia o usuário das instâncias. Para obter mais informações, consulte the section called “Desassociar usuários de uma instância”.
- Um usuário só é contado uma vez. Você é cobrado por usuário pelo Microsoft Office e pelo Visual Studio, independentemente do número de instâncias do EC2 às quais o usuário se conecta. Os usuários são cobrados pela assinatura uma vez, independentemente do uso de várias instâncias.

Solucionar problemas de status de assinatura inativa do Marketplace

Depois de configurar seu diretório com os produtos necessários, você precisaria assinar os produtos necessários. Os produtos com status de assinatura do Marketplace como Inativa exigem que você assine antes de poder associar usuários a uma instância e utilizá-los.

Solucione problemas de limites de usuários por instância

Há um limite de 25 instâncias por usuário. Caso precise de ajustes, entre em contato com o AWS Support. Os usuários são cobrados pela assinatura uma vez, independentemente do uso de várias instâncias.

Solucionar problemas do token CAL não vendido após a migração para o RDS SAL

Se você usa seus próprios servidores de licenças Microsoft RDS, todos os tokens de Licença de Acesso para Cliente (CAL) já emitidos permanecerão válidos até expirarem. Durante esse período, os usuários com tokens CAL válidos não são automaticamente inscritos no produto RDS SAL. Novas sessões de usuário não são automaticamente inscritas no RDS SAL, mesmo que o License Manager esteja configurado. O License Manager não substitui os tokens CAL existentes emitidos por seus próprios servidores de licenças. O servidor de licenças gerenciadas pelo serviço começa a emitir tokens e a lidar com novas solicitações somente após a expiração dos tokens CAL existentes. Quando os tokens CAL emitidos atualmente atingem sua data de expiração, as novas solicitações de token são tratadas pelo servidor de licenças gerenciado pelo serviço e os usuários são assinados automaticamente no produto RDS SAL conforme necessário.

A união perfeita de domínios não funciona para instâncias do EC2 com produtos de assinatura de usuário

O License Manager precisa realizar a associação de domínio nessas instâncias usando SSM para permitir acesso autorizado somente aos usuários inscritos no produto. Como resultado, o recurso de associação perfeita ao domínio é desativado.

O VPC endpoint foi criado em minha conta

O License Manager cria VPC endpoints necessários para que seus recursos se conectem aos servidores de ativação e permaneçam em conformidade quando você configura sua VPC.

Remova todos os recursos de VPC endpoint criados pelo License Manager

Para excluir os recursos do VPC endpoint, você deve realizar as seguintes ações:

- Desassociar todos os usuários das assinaturas baseadas no usuário. Para obter mais informações, consulte the section called “Desassociar usuários de uma instância”.
- Remova qualquer diretório que esteja configurado das configurações do License Manager. Para obter mais informações, consulte the section called “Cancelar o registro do Active Directory”.
- Terminar todas as instâncias que fornecem produtos de assinatura baseada no usuário. Para obter mais informações, consulte the section called “Execute uma instância a partir de uma licença incluída (AMI)”.

Alterar um nome de usuário no Managed Active Directory

Alterar um nome de usuário não afeta sua capacidade de RDP em instâncias associadas. Os usuários associados devem poder usar seus detalhes de login atualizados para RDP em instâncias de assinatura de usuário.

Dissociar usuários de uma instância encerrada

Sempre que uma instância de assinatura de usuário é encerrada, todos os usuários associados à instância são desassociados. Você não precisa desassociar manualmente o usuário.

> **Note**
>
> Os usuários não são dissociados se a instância for interrompida.

Instale software adicional em instâncias de assinatura de usuários

É possível instalar software adicional em suas instâncias que não estejam disponíveis como assinaturas baseadas no usuário. Instalações adicionais de software não são monitoradas pelo License Manager. Essas instalações devem ser realizadas usando a conta Admin, que é criada por padrão em seu AWS Managed Microsoft AD diretório. Para obter mais informações, consulte Conta de administrador no Guia de Directory Service administração.

Para instalar software adicional com a conta Admin, você deve:

- Inscrever a conta de administrador no produto fornecido pela instância.
- Associar a conta de administrador à instância.
- Conectar-se à instância usando a conta Admin para realizar a instalação.

Para obter mais informações, consulte the section called “Conceitos básicos”.

Pacotes de idioma japonês em instâncias de assinatura de usuários

A instalação do pacote de idioma japonês é compatível com instâncias de assinatura de usuário.

Usuário administrador local em instâncias de assinatura de usuário

Só permitimos que usuários sob o domínio do Active Directory gerenciado por usuários sejam associados a instâncias de assinatura de usuários para impedir o acesso não autorizado a esses

produtos da Microsoft. Quando você cria usuários locais com privilégios de administrador em instâncias que fornecem assinaturas baseadas em usuários, o status de integridade da instância muda para não íntegro.

Número de usuários que podem usar RDP para uma instância de assinaturas de usuários

As instâncias que fornecem assinaturas baseadas em usuário oferecem suporte a até duas sessões de usuário ativas por vez, conforme declarado em Use License Manager, assinaturas baseadas em usuário para produtos de software compatíveis. Por padrão, o Windows permite até duas conexões de área de trabalho remota, incluindo uma conexão de administrador a qualquer momento, em todas as edições do Windows Server. Para usar mais de 2 usuários simultâneos, os clientes precisam configurar um servidor de licenciamento RDS.

Usuários em meus produtos autogerenciados do AD para Office e Visual Studio

Para associar usuários em seu diretório autogerenciado, você deve estabelecer uma relação de confiança bidirecional entre seu diretório autogerenciado e seu diretório. AWS Managed Microsoft AD Para obter mais informações, consulte Tutorial: Crie uma relação de confiança entre seu domínio autogerenciado do Active Directory AWS Managed Microsoft AD e o seu no Guia de Directory Service Administração.

Sistemas operacionais Windows compatíveis

Para obter informações sobre plataformas de sistema operacional Windows suportadas, consultethe section called “Assinaturas de software compatíveis”.

Versões compatíveis do Office e do Visual Studio

Para obter informações sobre o software compatível com assinaturas baseadas no usuário, consulte. the section called “Software compatível”

Usando a assinatura de usuário com versões mais antigas do Windows Server

Quando você executa uma instância de uma AMI que oferece suporte ao Office LTSC Professional Plus, Office LTSC Standard ou Microsoft Visual Studio, a execução usa como padrão a versão mais recente da plataforma do sistema operacional Windows da AMI (por exemplo, Windows Server 2022). Para iniciar com uma versão anterior da plataforma do sistema operacional, siga estas etapas:

1. Abra o AWS Marketplace console emhttps://console.aws.amazon.com/marketplace.

2. No painel de navegação, escolha Gerenciar assinaturas.
3. Para otimizar os resultados da assinatura, você pode pesquisar todo ou parte do nome da assinatura. Por exemplo, Office LTSC Professional Plus, Office LTSC Standard ou Visual Studio Enterprise.
4. Selecione Iniciar nova instância no painel de assinatura. Isso abre uma página de configuração de execução.
5. Para iniciar uma instância a partir de uma AMI baseada em uma versão anterior da plataforma do sistema operacional Windows, selecione o link completo AWS Marketplace do site, localizado abaixo da versão do software. Isso leva você a uma página de configuração na qual você pode selecionar em uma lista de versões.
6. A lista mostra as versões mais recentes da AMI para as plataformas de sistema operacional Windows compatíveis. Selecione a versão do sistema operacional Windows a partir da qual você deseja iniciar.

Usando assinaturas de usuário do License Manager em todas as contas ou regiões

Esses cenários são suportados:

- Usando assinaturas de usuário do License Manager em todas as contas
- Usando assinaturas de usuário do License Manager com o Active Directory compartilhado

Esses cenários não são suportados:

- Usando assinaturas de usuário do License Manager em todas as regiões

Dicas para entrar em contato com o AWS Support

- Ao entrar em contato com o AWS suporte, crie uma instância com as mesmas configurações de uma instância encerrada e ative a proteção contra encerramento da instância para obter uma resposta rápida.
- Para qualquer problema relacionado ao RDP, precisaríamos de registros relacionados ao RDP para ajudar a depurar esses problemas. Utilize o 'AWSSupport-RunEC2RescueForWindowsTool' para ambientes com acesso à Internet. Para obter mais informações, consulte EC2Rescue for Windows Server.

- Ao usar uma instância do Office como instância de trabalho e montar um volume restaurado a partir de um instantâneo do volume da instância original, é possível coletar dados mesmo em um ambiente sem acesso à Internet.
- Solução de problemas de lançamentos de instâncias a partir do backup AMIs: se você iniciar uma instância a partir de uma AMI de backup, deverá encerrar a instância original.

Gerencie assinaturas Linux no License Manager

Com AWS License Manager, você pode visualizar e gerenciar assinaturas comerciais do Linux que suas instâncias do Amazon EC2 usam. Você pode monitorar a utilização de suas assinaturas Linux para as contas Regiões da AWS e AWS Organizations que você definiu em suas configurações. O License Manager oferece uma visão abrangente de suas instâncias em execução que usam assinaturas Linux. Também indica quando uma instância tem mais de uma assinatura definida.

Os dados que o License Manager descobre são agregados e exibidos no console do License Manager e no painel da Amazon CloudWatch . Você também pode acessar seus dados de assinatura por meio da AWS CLI API de assinatura Linux do License Manager ou associada SDKs.

As assinaturas de licenças do Linux podem vir das seguintes fontes:

Assinatura incluída AMIs

- Red Hat Enterprise Linux (RHEL)
- Modelo RHEL BYOS (Bring Your Own Subscription model) com o Red Hat Cloud Access Program
- SUSE Linux Enterprise Server
- AMI incluída na assinatura do Ubuntu Pro

Provedores de assinatura de terceiros

- Assinatura RHEL do Red Hat Subscription Manager (RHSM)

A descoberta de assinaturas do Linux usa o modelo de consistência eventual. Um modelo de consistência determina a maneira e o tempo em que os dados são carregados e apresentados na visualização de assinaturas do Linux. Com esse modelo, o License Manager garante que seus dados de assinatura do Linux sejam atualizados periodicamente a partir de seus recursos. Caso alguns dados não sejam ingeridos durante esses intervalos, as informações são fornecidas na próxima

emissão métrica. Esse comportamento pode atrasar a exibição de atributos, como instâncias Linux comerciais do EC2 recém-lançadas, no painel de assinaturas do Linux.

> **Note**
>
> Pode levar até 36 horas para que a descoberta inicial de atributos seja concluída e até 12 horas para que as instâncias recém-lançadas sejam descobertas e relatadas. Depois que seus recursos são descobertos, as CloudWatch métricas da Amazon são emitidas de hora em hora para dados de assinaturas Linux.

Se suas contas estiverem ativas AWS Organizations, você poderá registrar uma conta de membro como administrador delegado. Para obter mais informações, consulte Configurações de administrador delegado no License Manager.

Assinaturas duplicadas detectadas

Quando o License Manager detecta duas assinaturas Linux na mesma instância do EC2, ele define o alerta de assinatura duplicada. Você pode visualizar e filtrar dados de assinatura do Linux na página Instâncias no console do License Manager.

Instâncias do Red Hat Enterprise Linux 7 Extended Lifecycle Support (RHEL 7 ELS): quando você executa uma instância a partir de uma AMI incluída na assinatura para o RHEL 7 ELS, você ainda deve registrar sua instância na Red Hat e consumir uma autorização. Nesse caso, o License Manager relata uma assinatura duplicada, mas esse é o comportamento esperado.

Outras instâncias do Red Hat Linux: recomendamos que você pesquise o inventário de assinaturas no Red Hat Hybrid Cloud Console para descobrir quais assinaturas sua instância consome.

Tópicos adicionais

- Configurar a descoberta de assinaturas do Linux no License Manager
- Veja os dados da instância descoberta no License Manager
- Informações de cobrança para assinaturas Linux no License Manager
- Gerencie CloudWatch alarmes da Amazon para assinaturas Linux no License Manager

Configurar a descoberta de assinaturas do Linux no License Manager

Você pode configurar a descoberta de assinaturas Linux por meio do console do License Manager AWS CLI, da API de assinatura Linux do License Manager ou da API associada. SDKs Ao ativar a descoberta de assinaturas Linux para o Regiões da AWS que você especifica, você pode, opcionalmente, estender a descoberta às suas contas em. AWS Organizations Se você não quiser mais monitorar a utilização da assinatura, você também pode desativar a descoberta.

> **Note**
>
> Você pode descobrir e exibir até 5.000 recursos por conta, Região da AWS por padrão. Para solicitar um aumento desse limite, use o Formulário de aumento de limite.

Tópicos

Configurar a descoberta de assinaturas do Linux

Para configurar a descoberta de assinaturas do Linux na página Configurações no console do License Manager, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, selecione Configurações. Isso abre a página Configurações.
3. Abra a guia Assinaturas Linux e escolha Configurar. Isso abre o painel Configurar configurações de assinaturas Linux.
4. Selecione a Fonte em Regiões da AWS que a descoberta de assinaturas do Linux deve ser executada.
5. Para agregar dados de assinatura em todas as suas contas em AWS Organizations, selecione Link AWS Organizations. Essa opção só aparece se AWS Organizations estiver configurada para sua conta.
6. Analise e reconheça a opção que concede AWS License Manager permissão para criar uma função vinculada ao serviço para assinaturas Linux.

7. Escolha Save configuration.

Ative a descoberta de assinaturas do Red Hat Subscription Manager

Para recuperar informações de assinatura do Red Hat Subscription Manager (RHSM) em seu nome, o License Manager deve fornecer as credenciais da API da sua conta de cliente Red Hat.

Pré-requisitos

Antes de ativar a descoberta de assinaturas, verifique se você atendeu aos seguintes pré-requisitos.

- A descoberta padrão para assinaturas Linux deve ser ativada para você Conta da AWS antes que você possa configurar a descoberta de assinaturas do RHSM. Se a descoberta padrão não estiver ativada, consulteConfigurar a descoberta de assinaturas do Linux.
- Se você usa um login corporativo da Red Hat fornecido pelo administrador da organização, certifique-se de que seu ID de login tenha as seguintes funções e permissões atribuídas:
  - Função: Gerenciar suas assinaturas
  - Permissões:`View All`, ou `View/Edit All`

  Se sua ID de login não tiver as funções e permissões necessárias, entre em contato com o Administrador da Organização do portal Red Hat e solicite que ela seja adicionada ao seu login. Para obter mais informações sobre funções e permissões da Red Hat, consulte Funções e permissões do Red Hat Customer Portal. Para obter mais informações sobre como entrar em contato com o administrador da organização do Red Hat Portal, consulte Como eu sei quem é meu administrador da organização? na base de conhecimento do Red Hat Customer Portal.
- Para ativar a descoberta da assinatura do RHSM, você deve fornecer o token offline da API da conta do cliente Red Hat ou um AWS Secrets Manager segredo que contenha o token offline. Para obter seu token offline, siga as etapas descritas em Geração de um novo token offline no site de documentação da Red Hat.

> **Important**
>
> Sua segurança é importante para nós. Seu token de acesso off-line da Red Hat é armazenado com segurança no Secrets Manager. O License Manager usa seu segredo para gerar um token de acesso temporário sempre que solicita detalhes da assinatura da Red Hat.

Ativação

Para ativar a descoberta do RHSM na página Configurações no console do License Manager, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, selecione Configurações.
3. Na página Configurações, abra a guia Assinaturas Linux.
4. Escolha Editar para atualizar suas configurações de assinatura do Linux. Isso abre a página de descoberta de Configurar assinaturas Linux.
5. Para iniciar o processo de ativação, marque a caixa de seleção Ativar a descoberta do Red Hat Subscription Manager (RHSM). Isso exibe o painel Vincular conta RHSM.
6. Selecione a opção Segredo (Token) que se aplica ao seu segredo e siga as etapas restantes que dependem da opção escolhida.
7. Opção: criar um novo segredo — recomendado

   Forneça o token de acesso off-line da Red Hat e deixe o License Manager criar o segredo de acesso no Secrets Manager em seu nome.

   a. Insira um nome para seu segredo em Nome secreto.
   b. Cole seu token de acesso off-line da Red Hat na caixa de token offline. Certifique-se de que não haja espaços extras ou quebras de linha antes ou depois do valor do token. Você pode gerar seu token de acesso off-line da Red Hat na página Red Hat Subscription Manager API Tokens.

   Opção: Selecione um segredo

   Selecione um segredo existente no Secrets Manager que contenha seu token de acesso offline da Red Hat.
8. (opcional) Adicione tags para seu segredo.
9. Selecione a caixa de seleção na parte inferior da página para reconhecer que, ao ativar a descoberta do Red Hat Subscription Manager, você concede acesso ao AWS License Manager serviço para coletar dados relacionados às assinaturas da Red Hat usadas nas instâncias do Amazon EC2.
10. Selecione Ativar.

Motivos de status da descoberta de atributos

AWS License Manager exibirá um status e um motivo de status correspondente para cada um Região da AWS que você escolher para habilitar a descoberta para assinaturas Linux. O motivo do status variará se você tiver vinculado assinaturas Linux com: AWS Organizations

- In progress (Em andamento)
- Com êxito
- Failed

O motivo do status exibido para cada região que você escolher mostrará até dois motivos de status por vez. A tabela a seguir oferece mais detalhes:

Ação de motivo de status	Description
Account-onboard	Integração em uma única conta.
Account-offboard	Não integração em uma única conta.
Org-onboard	Integração de uma organização inteira.
Org-Offboard	Não integração de uma organização inteira.

É possível chamar a API `UpdateServiceSettings` e, posteriormente, chamar a API `GetServiceSettings` para monitorar o progresso da habilitação das assinaturas Linux. Cada status e motivo de status podem ser aplicados a várias regiões ao mesmo tempo. A tabela a seguir fornece mais detalhes sobre o status e o motivo do status:

Status	Motivo do status	Description
Em andamento	`"Region": "Account-Onboard: Pending"`	A habilitação de assinaturas Linux para uma única conta está em andamento.

Status	Motivo do status	Description
	`"Region": "Org-Onboard: Pending"`	A habilitação de assinaturas Linux para uma organização está em andamento.
	`"Region": "Account-Offboard: Pending`	A desabilitação de assinaturas Linux para uma única conta está em andamento.
	`"Region": "Org-Offboard: Pending`	A desabilitação de assinaturas Linux para uma organização está em andamento.
Com êxito	`"Region": "Account-Onboard: Successful"`	A habilitação de assinaturas Linux para uma única conta foi bem-sucedida.
	`"Region": "Org-Onboard: Successful"`	A habilitação de assinaturas Linux para uma organização foi bem-sucedida.
	`"Region": "Account-Offboard: Successful`	A desabilitação de assinaturas Linux para uma única conta foi bem-sucedida.
	`"Region": "Org-Offboard: Successful`	A desabilitação de assinaturas Linux para uma organização foi bem-sucedida.
Failed	`"Region": "Account-Onboard: Failed - Service-linked role not present"`	A ativação de assinaturas Linux para uma única conta falhou porque não foi criada o perfil vinculado ao serviço, que é obrigatória. Crie o perfil necessário e tente novamente.

Status	Motivo do status	Description
	`"Region": "Account-Onboard: Failed - An internal error occurred"`	A ativação de assinaturas do Linux para uma única conta falhou devido a um erro interno.
	`"Region": "Org-Onboard: Failed - Account isn't the management account"`	A habilitação de assinaturas Linux para uma organização falhou porque a conta que executa a operação não é a conta de gerenciamento da organização. Faça login na conta de gerenciamento e tente novamente.
	`"Region": "Org-Onboard: Failed - Account isn't part of an  organization"`	A habilitação de assinaturas Linux para uma organização falhou porque a conta que executa a operação não pertence à organização. Experimente a operação a partir de uma conta da organização ou adicione essa conta à organização e tente novamente.
	`"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"`	A habilitação de assinaturas Linux para uma organização falhou porque o License Manager não ter as permissões para acessar a organização. Crie um perfil vinculado ao serviço para assinaturas do Linux e tente novamente.

Desative a descoberta de assinaturas Linux

Você pode desativar a descoberta de assinaturas Linux na página de configurações. AWS License Manager No entanto, se você ativou a descoberta para

> **Warning**
>
> Se você desativar a descoberta, todos os seus dados descobertos anteriormente para assinaturas Linux serão removidos do. AWS License Manager

Para desabilitar a descoberta de assinaturas Linux

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, escolha a guia Assinaturas Linux e escolha Desativar descoberta de assinaturas Linux.
4. Digite **`Disable`** e escolha Desativar para confirmar a desativação.
5. (Opcional) Remover o perfil vinculado ao serviço usada para assinaturas do Linux. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço para o License Manager.
6. (Opcional) Desative o acesso confiável entre o License Manager e sua organização. Para obter mais informações, consulte AWS License ManagerAWS Organizations e.

Veja os dados da instância descoberta no License Manager

Depois que o License Manager concluir o processo inicial de descoberta de recursos no seu selecionado Regiões da AWS, você poderá visualizar os resultados no console. Se você optar por vincular AWS Organizations, o License Manager agrega dados de contas em toda a sua organização. Para ver uma lista de instâncias com assinaturas que atendem aos seus critérios de filtro, navegue até a seção Instâncias do AWS License Manager console. A lista exibe os seguintes campos principais.

- ID da instância – a ID da instância.
- Status – o status da instância.
- Tipo da instância – o tipo da instância.
- Assinatura — O nome da assinatura de licença que a instância usa.
- Alerta de duplicatas — Indica que você tem duas assinaturas de licença diferentes para o mesmo software na sua instância.
- ID da conta – a ID da conta proprietária da instância.
- Região — A região Região da AWS em que a instância reside.

- ID do AMI – a ID do AMI usado para executar a instância.
- Operação de uso – a operação da instância e o código de faturamento associado à AMI. Para obter mais informações, consulte Valores da operação de uso.
- Código do produto – O código do produto associado ao AMI usado para executar a instância. Para obter mais informações, consulte Códigos do produto AMI.
- LastUpdatedTime— A hora em que a última descoberta atualizou os detalhes da instância.

Tópicos

Visualize dados de todas as instâncias

Você pode visualizar e filtrar os dados de assinatura do Linux que o License Manager descobriu para as instâncias em sua conta ou AWS Organizations, da seguinte forma.

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Instâncias. Isso exibe uma lista de instâncias com dados de assinatura do Linux.
3. (Opcional) Você pode usar os seguintes filtros para otimizar seus resultados:
   - Conta
   - ID DA AMI
   - Assinatura duplicada
   - ID da instância
   - Região
   - Código do produto
   - Operação de uso
4. (Opcional) Escolha Exportar visualização como CSV para exportar dados de todas as instâncias como um arquivo de valores separados por vírgula (CSV).

Visualize dados de instâncias por assinatura

É possível ver os dados de todas as instâncias que foram agregados em todas as contas da organização, nas regiões escolhidas.

Para visualizar dados descobertos por instâncias com uma assinatura específica

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura da qual você gostaria de ver os dados.
4. Escolha a guia Instâncias e revise os dados conforme necessário no console. É possível filtrar os dados por:
   - ID da instância
   - Conta
   - Região
   - ID DA AMI
   - Operação de uso
   - Código do produto
5. (Opcional) Escolha Exportar visualização como CSV para exportar dados das instâncias com essa assinatura como um arquivo de valores separados por vírgula (CSV).

Informações de cobrança para assinaturas Linux no License Manager

Cada assinatura comercial do Linux executada no Amazon EC2 tem informações de cobrança associadas à Amazon Machine Image (AMI). As assinaturas comerciais do Linux têm a operação de uso do Amazon EC2 AWS Marketplace , o código do produto ou uma combinação de ambos. Para obter mais informações, consulte os campos de informações de cobrança do AMI no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux e os códigos do produto AMI no Guia do vendedor do AWS Marketplace .

Nome da assinatura	Operação de uso do Amazon EC2	AWS Marketplace código do produto	Tipo de assinatura
Red Hat Enterprise Linux Server BYOS	RunInstances0:00g	✗	Traga seu próprio modelo de assinatura (BYOS)
Red Hat Enterprise Linux Server	RunInstances00:10	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com complemento de alta disponibilidade	RunInstances:1010	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com SQL Server Standard e alta disponibilidade	RunInstances:1014	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com SQL Server Enterprise e alta disponibilidade	RunInstances: 1110	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com SQL Server Standard	RunInstances00:14	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com SQL Server Web	RunInstances02:10	✗	Assinatura EC2 incluída
Red Hat Enterpris e Linux com SQL Server Enterprise	RunInstances01:10	✗	Assinatura EC2 incluída

Nome da assinatura	Operação de uso do Amazon EC2	AWS Marketplace código do produto	Tipo de assinatura
SUSE Linux Enterprise Server	RunInstances: 000g	✗	Assinatura EC2 incluída
Red Hat Enterprise Linux para SAP com alta disponibilidade e serviços de atualização	RunInstances00:10	✓	AWS Marketplace assinatura [1]
SUSE Linux Enterprise Server com SAP	✗	✓	AWS Marketplace Assinatura
Ubuntu Pro	RunInstances0g00	✓	AWS Marketplace Assinatura
Workstation do Red Hat Enterprise Linux	✗	✓	AWS Marketplace Assinatura

[1] Essa assinatura tem uma operação de uso do Amazon EC2 e um código de AWS Marketplace produto.

Métricas de uso para assinaturas Linux

As seguintes métricas e dimensões estão disponíveis para assinaturas Linux:

Métrica	Description
RunningInstancesCount	O número total de instâncias em execução na conta atual agrupadas pelo nome da assinatura ou, pelo nome da assinatura e região. Unidades: contagem Dimensões: `SubscriptionName` : o nome da assinatura.

Métrica	Description
	`Region`: a região em que o atributo usando uma assinatura comercial do Linux foi descoberto.

Gerencie CloudWatch alarmes da Amazon para assinaturas Linux no License Manager

A página da lista de assinaturas Linux no console do License Manager mostra os seguintes detalhes importantes, incluindo os CloudWatch alarmes da Amazon que você configurou para cada assinatura Linux que o License Manager encontrou em suas instâncias.

- Nome da assinatura
- Tipo de assinatura
- Número de instâncias em execução por assinatura
- CloudWatch Alarmes configurados da Amazon

Quando você escolhe uma assinatura Linux na página da lista, a guia Métricas de uso e alarmes exibe os dados dessa assinatura. Nessa guia, os CloudWatch painéis da Amazon são exibidos para a assinatura escolhida no console do License Manager. Você pode ajustar o painel para abranger um determinado período ou intervalo de avaliação, em horas, dias ou uma semana a partir de uma data selecionada.

Na guia Métricas de uso e alarmes, cada assinatura tem uma seção Alarmes com os seguintes detalhes:

- Nome do alarme – O nome do alarme.
- Estado – o estado do alarme.
- Dimensão – as dimensões do alarme. A dimensão incluirá o tipo de instância Região da AWS e que foi definido.
- Condição – a condição do alarme. A condição incluirá o operador de comparação e o valor limite de alarme que foi definido.

Você pode criar CloudWatch alarmes usando as dimensões e condições definidas para rastrear e alertar com base na utilização atual da sua assinatura. O console de assinaturas do Linux exibe um

resumo dos nomes de assinatura em uso, os tipos de assinatura, a quantidade de instâncias em execução de cada uma e o status do alarme.

A seguir estão os possíveis estados CloudWatch de alarme:

- OK – a métrica ou a expressão está dentro do limite definido.
- ALARME – a métrica ou a expressão está fora do limite definido.
- DADOS INSUFICIENTES – o alarme acabou de ser acionado, a métrica não está disponível ou não há dados suficientes para a métrica determinar o estado do alarme.

Tópicos

Crie um CloudWatch alarme para assinaturas Linux

É possível criar alarmes para cada assinatura comercial do Linux descoberta nas instâncias do EC2 em execução. Se necessário, é possível criar vários alarmes com diferentes dimensões e condições para cada assinatura.

Para criar um CloudWatch alarme para assinaturas Linux a partir do console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura para a qual criar um alarme e escolha Criar alarme.
4. Especifique o seguinte para o alarme:
   - Nome do alarme — especifique um nome que se assemelhe ao `AWS-LM-LS-AlarmName`.
   - Tipo de instância — escolha um tipo de instância que usará a assinatura selecionada.
   - Região de uso — escolha as regiões para as quais criar os alarmes.
   - Operador de comparação — o operador de comparação para o limite de alarme.
   - Valor do limite do alarme — o valor do limite do alarme.
5. Escolha Create para criar o alarme.

Modificar um CloudWatch alarme para assinaturas Linux

Você pode modificar CloudWatch os alarmes existentes no console do License Manager para se adaptar às mudanças nos requisitos.

Para modificar um CloudWatch alarme para assinaturas Linux a partir do console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura a ser modificada e escolha Editar.
4. Modifique os valores definidos conforme necessário.
5. Escolha Editar para modificar o alarme.

Excluir um CloudWatch alarme para assinaturas Linux

Você pode excluir CloudWatch os alarmes existentes do console do License Manager para se adaptar às mudanças nos requisitos.

Para excluir um CloudWatch alarme para assinaturas Linux do console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura a ser modificada e escolha Excluir.

Licenças emitidas pelo vendedor no License Manager

Fornecedores independentes de software (ISVs) podem usar AWS License Manager para gerenciar e distribuir licenças de software para usuários finais. Como emissor, você pode monitorar o uso das licenças emitidas centralmente usando o painel do License Manager.

O License Manager usa padrões abertos e seguros do setor para representar licenças e permite que os clientes verifiquem criptograficamente sua autenticidade. O License Manager associa cada licença a uma chave assimétrica. Como ISV, você possui as AWS KMS chaves assimétricas e as armazena em sua conta.

As licenças emitidas pelo vendedor exigem a replicação entre Regiões dos metadados da licença. O License Manager replica automaticamente cada licença emitida pelo vendedor e respectivas informações associadas para outras regiões.

O License Manager oferece suporte a uma variedade de modelos de licenciamento diferentes, incluindo os seguintes:

- Perpétuas — licenças vitalícias sem data de expiração, que autorizam os usuários a usar o software indefinidamente.
- Flutuantes — licenças que podem ser compartilhadas com várias instâncias do aplicativo. As licenças podem ser pré-pagas e um conjunto fixo de direitos pode ser adicionado a elas.
- Por assinatura — licenças com datas de expiração que podem ser renovadas automaticamente, a menos que sejam especificamente desativadas.
- Baseadas no uso — licenças com termos específicos baseados no uso, como o número de solicitações de API, transações ou atributos de armazenamento.

Você pode criar licenças no License Manager e distribuí-las aos seus clientes com uma identidade AWS IAM ou por meio de tokens portadores gerados pelo License Manager. Clientes ISV com uma AWS conta podem redistribuir os direitos de licença para AWS identidades em suas respectivas organizações. Clientes com direitos distribuídos podem fazer check-out e check-in dos direitos exigidos pela licença por meio de integração de seu software com o License Manager.

Direitos de licença emitidos pelo vendedor no License Manager

O License Manager captura os recursos da licença emitida pelo vendedor como direitos na licença. Os direitos podem ser caracterizados com uma quantidade limitada ou ilimitada. Um exemplo de direito limitado é ‘40 GB de transferência de dados’. Um exemplo de direito de quantidade ilimitada é o ‘Nível Platina‘.

Uma licença captura todos os direitos concedidos, as datas de ativação e expiração e os detalhes do emissor. Uma licença é uma entidade versionada e cada versão é imutável. As versões da licença são atualizadas sempre que a licença é alterada.

Para fazer o check-out ou o check-in de direitos limitados, os pedidos de ISV devem especificar o valor de cada capacidade limitada. Para direitos ilimitados, os pedidos de ISV podem simplesmente especificar o direito relevante para fazer o check-out ou fazer o check-in novamente. Por fim, os atributos limitados também oferecem suporte a um sinalizador de “excedente”, que indica se os

usuários finais podem exceder o uso dos direitos iniciais. O License Manager rastreia e relata o uso, bem como os excedentes, ao ISV.

Uso da licença emitida pelo vendedor no License Manager

O License Manager permite acompanhar centralmente as licenças em várias regiões, mantendo uma contagem de todos os direitos com check out. O License Manager também rastreia a identidade do usuário e o identificador de atributo subjacente, se disponível, associado a cada check out, além de quando o check-out foi feito. Você pode acompanhar esses dados de séries temporais por meio de CloudWatch Eventos.

As licenças podem estar em um dos seguintes estados:

- Criada — a licença foi criada.
- Atualizada — a licença está atualizada.
- Desativada — a licença está desativada.
- Excluída — a licença foi excluída.

Permissões necessárias para rastrear o uso da licença emitida pelo vendedor no License Manager

Para começar a usar esse atributo, você precisa de permissão para chamar as seguintes ações da API do License Manager.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenses",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
```

```
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:GetLicenseUsage",
            "license-manager:CreateGrant",
            "license-manager:CreateGrantVersion",
            "license-manager:DeleteGrant",
            "license-manager:GetGrant",
            "license-manager:ListDistributedGrants"
        ],
        "Resource": "*"
      }
    ]
}
```

Se você fizer a integração com o License Manager para que clientes sem uma AWS conta possam consumir licenças vendidas fora dele AWS Marketplace, você deverá criar uma função do IAM que permita que seu aplicativo de software chame a API do License Manager.

Se você usar o Console de gerenciamento da AWS para distribuir credenciais temporárias para clientes sem uma Conta da AWS, o License Manager criará automaticamente as `AWSLicenseManagerConsumptionRole` em seu nome. Para obter mais informações, consulte Obtenha credenciais temporárias para clientes ISV sem uma conta AWS. Para criar essa função a partir do AWS CLI, use o comando AWS IAM create-role, conforme mostrado no exemplo a seguir.

```
aws iam create-role
    --role-name AWSLicenseManagerConsumptionRole
    --description "Role used to consume licenses using AWS License Manager"
    --max-session-duration 3600
    --assume-role-policy-document file://trust-policy-document.json
```

O `trust-policy-document.json` arquivo fornecido deve ser semelhante ao exemplo a seguir, com seu próprio Conta da AWS ID substituído como a conta do emissor do token.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Federated": "openid-license-manager.amazonaws.com"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "openid-license-manager.amazonaws.com:amr": "aws:license-
manager:token-issuer-123456789012:123456789012"
                }
            }
        }
    ]
}
```

Em seguida, use o attach-role-policycomando para adicionar a política AWSLicenseManagerConsumptionPolicy AWS gerenciada à AWSLicenseManagerConsumptionRolefunção.

```
aws iam attach-role-policy
    --policy-arn arn:aws:iam::aws:policy/service-role/
AWSLicenseManagerConsumptionPolicy
    --role-name AWSLicenseManagerConsumptionRole
```

Crie licenças emitidas pelo vendedor no License Manager

Use o procedimento a seguir para criar um bloco de licenças para conceder aos clientes que usam o Console de gerenciamento da AWS. Como alternativa, você pode criar a licença usando a ação CreateLicenseda API.

Para criar uma licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha Criar licença.
4. Para Metadados de licença, forneça as seguintes informações:
   - Nome da licença — o nome, com até 150 caracteres, a ser exibido aos compradores.
   - Descrição da licença — uma descrição opcional, de até 400 caracteres, que diferencia essa licença de outras licenças.

- SKU do produto — o SKU do produto.
- Destinatário — o nome do destinatário (empresa ou pessoa física).
- Região de origem — A AWS região da licença. Embora as licenças possam ser consumidas globalmente, as licenças somente podem ser alteradas na região de origem. Não é possível alterar a região de origem de uma licença depois de criá-la.
- Data de início da licença — a data de ativação.
- Data de término da licença — a data de término da licença, se aplicável.

5. Para Configuração de consumo, forneça as seguintes informações:

   - Frequência de renovação — se deve o consumo deve ser renovado semanalmente, mensalmente ou não deve ser renovado.
   - Configuração de consumo — escolha Opções de configuração de consumo provisório se a licença for usada para conectividade contínua ou Empréstimo se a licença for usada offline. Insira Tempo máximo de vida (minutos) para definir a duração da disponibilidade da licença.

6. Para Emissor, forneça as seguintes informações:

   - Insira uma AWS KMS chave — o License Manager usa essa chave para assinar e verificar o emissor. Para obter mais informações, consulte Assinatura criptográfica de licenças no License Manager.
   - Nome do emissor — o nome comercial do vendedor.
   - Vendedor registrado — um nome comercial opcional.
   - URL do contrato — o URL do contrato de licença.

7. Para Direitos, forneça as seguintes informações sobre os atributos que a licença concede aos destinatários:

   - Nome – o nome do destinatário.
   - Tipo de unidade — selecione o tipo de unidade e, em seguida, forneça a contagem máxima.
   - Marque Permitir check-in se os destinatários precisarem fazer o check-in das licenças antes da renovação.
   - Marque Excedentes permitidos se os destinatários puderem usar o atributo além da contagem máxima. Essa opção pode gerar cobranças adicionais para o destinatário.

8. Escolha Criar licença.

Conceda licenças emitidas pelo vendedor do License Manager para clientes ISV

Depois de adicionar a nova licença, você pode conceder a licença a um cliente com uma conta da AWS usando o Console de gerenciamento da AWS. O destinatário deve aceitar a concessão antes de usar a licença. Para obter mais informações, consulte Licenças concedidas no License Manager.

Como alternativa, se o cliente não tiver uma AWS conta, você pode usar a API License Manager para permitir que os clientes consumam licenças.

Para conceder uma licença a um cliente usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha a ID da licença para abrir a página de detalhes.
4. Em Concessões, escolha Criar concessão.
5. Para Detalhes da concessão, forneça as seguintes informações:
   - Nome da concessão — o nome da concessão. Isso é usado para ativar os atributos de pesquisa.
   - AWS ID da conta — O número da AWS conta do destinatário da licença.
   - Direitos da licença
     - Selecione Consumo se o destinatário puder consumir os direitos concedidos.
     - Selecione Distribuição se o destinatário puder distribuir os direitos concedidos para outras AWS contas.
     - Selecione Permitir geração de token local para autenticar licenças compartilhadas sem usar AWS identidades ou credenciais.
     - Selecione Permitir envio de registros de uso para permitir que os destinatários da licença emitam registros de uso para tipos de uso.
   - Região de origem — A Região da AWS para a licença.
6. Escolha Criar concessão.

Obtenha credenciais temporárias para clientes ISV sem uma conta AWS

Para clientes sem uma AWS conta, você pode usar os direitos da mesma forma que usa para seus clientes com uma AWS conta. Use o procedimento a seguir para obter AWS credenciais temporárias para seus clientes sem uma AWS conta. As chamadas de API devem ser feitas na região de origem.

Para obter credenciais temporárias para usar na chamada da API do License Manager

1. Chame a ação CreateTokenda API para obter um token de atualização codificado como um token JWT.
2. Chame a ação da GetAccessTokenAPI, especificando o token de atualização que você recebeu `CreateToken` na etapa anterior, para receber um token de acesso temporário.
3. Chame a ação da AssumeRoleWithWebIdentityAPI, especificando o token de acesso que você recebeu `GetAccessToken` na etapa anterior e a AWSLicenseManagerConsumptionRolefunção que você criou para obter AWS credenciais temporárias.

Para criar um token a partir do AWS License Manager console

1. No console do License Manager, navegue até a página de detalhes da licença para ver o direito de licença específico que você deseja usar sem uma AWS conta.
2. Escolha Criar token para gerar um token de acesso temporário.

> **Note**
>
> Na primeira vez que gerar um token de acesso temporário, deverá criar um perfil de serviço para que o License Manager possa acessar os serviços em seu nome. O seguinte perfil de serviço será criado: `AWSLicenseManagerConsumptionRole`.

3. Faça o download do arquivo do `token.csv` ou copie a string do token quando ela for gerada.

> **Important**
>
> Esta é a única vez que você poderá visualizar ou baixar esse token. Recomendamos que baixe o token e armazene o arquivo em um lugar seguro. Você pode criar novos tokens a qualquer momento, até o limite do serviço.

Confira as licenças emitidas pelo vendedor no License Manager

O License Manager permite que vários usuários consumam simultaneamente direitos, com atributos limitados, de uma única licença. Chame a ação de API CheckoutLicense. A seguir, está uma descrição dos parâmetros.

- Impressão digital da chave — emissor de licenças confiável.

  Exemplo: aws:123456789012:issuer:issuer-fingerprint

- SKU do produto — o identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs. Portanto, impressões digitais confiáveis desempenham um papel importante.

  Exemplo: 1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE

- Direitos — capacidades para fazer check-out. Se você especificar uma capacidade ilimitada, a quantidade será zero. Exemplo:

```
"Entitlements": [
    {
        "Name": "DataTransfer",
        "Unit": "Gigabytes",
        "Value": 10
    },
    {
        "Name": "DataStorage",
        "Unit": "Gigabytes",
        "Value": 5
    }
]
```

- Beneficiário — O Software as a Service (SaaS ISVs) pode verificar as licenças em nome de um cliente incluindo o identificador do cliente. O License Manager limita a chamada ao repositório de licenças criadas na conta SaaS do ISV.

  Exemplo: user@domínio.com.br

- ID do nó — um identificador usado para bloquear a licença a uma única instância do aplicativo.

  Exemplo: 10.0.21.57

Excluir licenças emitidas pelo vendedor no License Manager

Depois de excluir uma licença, você pode recriá-la. A licença e seus dados são retidos e disponibilizados para o emissor e os detentores da licença no modo somente leitura por seis meses.

Use o procedimento a seguir para excluir uma licença que você criou usando o Console de gerenciamento da AWS. Como alternativa, você pode excluir a licença usando a ação DeleteLicenseda API.

Para excluir uma configuração de licença usando o console

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha o botão de opção ao lado da licença para selecioná-la para exclusão.
4. Escolha Excluir. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Configurações no License Manager

A seção Configurações do AWS License Manager console exibe as configurações da conta atual. Você deve definir as configurações para ativar a funcionalidade associada.

Managed licenses

As configurações a seguir são configuráveis para licenças gerenciadas:

- Distribuição de direitos gerenciados e licenças autogerenciadas para sua organização
- Descoberta de atributos entre contas
- Notificação do Amazon SNS
- Descoberta de ativos de licença e configuração de conjunto de regras para grupos de ativos de licença

Para organizações que usam grupos de ativos de licenças, configurações adicionais estão disponíveis para descoberta entre regiões e gerenciamento de licenças em toda a organização em várias AWS regiões e contas.

Para obter mais informações, consulte Configurações de licença gerenciada no License Manager.

Linux subscriptions

As configurações a seguir são configuráveis para assinaturas Linux:

- Descoberta e agregação de dados de assinatura de licenças do Commercial Linux
- Descoberta do Red Hat Subscription Manager (RHSM) para assinaturas Linux

Para obter mais informações, consulte Configurações de assinatura do Linux no License Manager.

User-based subscriptions

As configurações a seguir são configuráveis para assinaturas baseadas no usuário:

- AWS Managed Microsoft AD
- Nuvem privada virtual (VPC)

Para obter mais informações, consulte Configurações de assinatura baseadas no usuário no License Manager.

Delegated administration

Essa guia será exibida se sua conta tiver acesso administrativo à sua organização. Como administrador, você pode registrar um administrador delegado a partir do AWS CLI ou Console de gerenciamento da AWS. Para obter mais informações, consulte Configurações de administrador delegado no License Manager.

Tópicos de configurações

- Editar configurações do License Manager
- Configurações de licença gerenciada no License Manager
  - Descoberta de ativos de licenças e configurações do conjunto de regras
  - Detalhes da conta
  - Descoberta de atributos entre contas
  - Simple Notification Service (SNS)
- Configurações de assinatura do Linux no License Manager
  - Configurações de assinaturas Linux

Editar configurações do License Manager

Para editar suas configurações do License Manager, siga estas etapas:

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Configurações.
3. Escolha a guia que contém as configurações a serem definidas. Por exemplo, escolha Licenças gerenciadas para configurar os Detalhes da conta.
4. Depois de definir suas configurações, escolha Salvar ou escolha Cancelar para voltar atrás.

Configurações de licença gerenciada no License Manager

As seguintes configurações estão disponíveis para as licenças gerenciadas.

Descoberta de ativos de licenças e configurações do conjunto de regras

Para organizações que usam grupos de ativos de licença, você pode definir a descoberta de ativos de licença e as configurações do conjunto de regras para permitir a descoberta entre regiões e o gerenciamento de licenças em toda a organização em várias regiões AWS e contas em suas Organizations. AWS

As configurações de descoberta de ativos de licença incluem:

- Configuração de descoberta de região para selecionar AWS regiões de origem para descoberta de software
- Configurações de descoberta em toda a organização para proprietários da organização

Detalhes da conta

Você pode revisar os detalhes da sua conta para ver informações como o tipo de conta, se as contas AWS Organizations estão vinculadas, o ARN do bucket S3 do License Manager da conta e o ARN do AWS Resource Access Manager compartilhamento. Esta seção também permite que você vincule suas AWS Organizations contas.

Para distribuir direitos gerenciados ou licenças autogerenciadas em sua organização, escolha Vincular contas. AWS Organizations As concessões distribuídas para direitos gerenciados são aceitas automaticamente por todas as contas de seus membros. Quando você seleciona essa opção, adicionamos um perfil vinculado ao serviço às contas de gerenciamento e de membro.

> **Note**
>
> Para ativar essa opção, faça login na sua conta de gerenciamento e ative todos os recursos AWS Organizations. Para obter mais informações, consulte Habilitar todos os recursos em sua organização no Manual do usuário do AWS Organizations .
> Essa seleção também cria um compartilhamento de AWS Resource Access Manager recursos em sua conta de gerenciamento, o que permite que você compartilhe facilmente licenças autogerenciadas. Para obter mais informações, consulte o Guia do usuário do AWS Resource Access Manager.

Para desativar essa opção, chame a UpdateServiceSettingsAPI.

Descoberta de atributos entre contas

É possível ativar a descoberta de atributos entre contas para gerenciar o uso da licença em todas as contas no AWS Organizations.

Para habilitar a descoberta de atributos entre contas em sua organização, escolha Ativar para descoberta de atributos entre contas. Quando você ativa a descoberta de recursos entre contas, ela AWS Organizations é automaticamente vinculada para realizar a descoberta de recursos em todas as suas contas.

O License Manager usa o inventário do Systems Manager para descobrir o uso de software. Verifique se configurou o inventário do SSM em todos os seus atributos. A consulta do inventário do Systems Manager exige o seguinte:

- Sincronização de dados de atributos para armazenar inventário em um bucket do Amazon S3.
- Amazon Athena para agregar dados de inventário de suas contas no AWS Organizations.
- AWS Glue para fornecer uma experiência de consulta rápida.

> **Note**
>
> As regiões de AWS partição comercial (aws) não exigem Amazon Athena nem AWS Glue consultam nem agregam dados de inventário do Systems Manager para descobrir o uso do software. No entanto, Amazon Athena elas ainda AWS Glue são necessárias para outras partições aws-us-gov, como as regiões aws-cn e aws-iso.

Simple Notification Service (SNS)

É possível configurar um Amazon SNS para receber notificações e alertas do License Manager.

Para configurar um tópico do Amazon SNS

1. Escolha Editar ao lado de Simple Notification Service (SNS).
2. Especifique um ARN do tópico do SNS no seguinte formato:

   ```
   arn:<aws_partition>:sns:<region>:<account_id>:aws-license-manager-service-*
   ```

3. Escolha Salvar alterações.

Configurações de assinatura do Linux no License Manager

Durante o processo de descoberta, o License Manager pesquisa as instâncias do EC2 que estão sendo executadas sob suas Conta da AWS assinaturas Linux. Ele detecta se você tem mais de uma assinatura Linux definida para qualquer instância e agrega os dados.

Configurações de assinaturas Linux

Você pode definir as configurações das assinaturas Linux para controlar como o License Manager lida com a descoberta e a agregação. As configurações padrão de descoberta se aplicam a todos os tipos de assinaturas Linux.

As ações a seguir estão disponíveis para configurar a descoberta de assinaturas do Linux.

Edite

Altere as configurações para descoberta de assinaturas do Linux.

Desativar

Desative a descoberta e a agregação de assinaturas Linux associadas às suas instâncias do EC2. Se você também tiver a descoberta ativada para o Red Hat Subscription Manager, o License Manager primeiro desativa seu provedor registrado no RHSM e, em seguida, continua com a desativação para descoberta de assinaturas Linux.

> **Note**
>
> A desativação não afeta seu segredo de acesso ao Red Hat Subscription Manager (RHSM). Para evitar cobranças em sua AWS fatura por um segredo associado que você não precisa mais, consulte Excluir um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário.

As configurações a seguir são exibidas no console do License Manager para descoberta de assinaturas do Linux.

Configurações de descoberta de assinaturas do Linux

Descoberta de assinaturas Linux

Indica se você ativou a descoberta de assinaturas Linux para sua conta.

Origem Regiões da AWS

Regiões da AWS onde você deseja que o License Manager descubra os dados da assinatura.

AWS Organizations

Opcionalmente, agregue dados de assinatura em todas as suas contas em. AWS Organizations

Para obter mais informações, consulte Gerencie assinaturas Linux no License Manager.

Descoberta do Red Hat Subscription Manager

Se você ativou a descoberta de assinaturas do Linux, você pode configurar o acesso ao License Manager para recuperar dados adicionais para assinaturas do RHEL que são gerenciadas por meio do Red Hat Subscription Manager (RHSM).

As ações a seguir estão disponíveis para configurar sua descoberta de assinatura do RHSM.

Editar tags

Altere as tags associadas ao seu segredo de acesso.

> **Note**
>
> Se precisar fazer outras alterações em sua assinatura do RHSM, primeiro desative seu registro atual e, em seguida, configure um novo registro.

Desativar

Desative seu provedor registrado no RHSM.

> **Note**
>
> A desativação não afeta seu segredo de acesso ao Red Hat Subscription Manager (RHSM). Para evitar cobranças em sua AWS fatura por um segredo associado que você não precisa mais, consulte Excluir um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário.

As configurações a seguir são exibidas no console do License Manager para descoberta do RHSM.

Configurações de descoberta do Red Hat Subscription Manager

Status da descoberta

Indica se você ativou a descoberta para assinaturas do RHSM.

Nome secreto

Links para o segredo de acesso do RHSM AWS Secrets Manager que contém seu token offline da Red Hat. O License Manager usa esse segredo para gerar um novo token de acesso temporário para solicitar dados de assinatura do Red Hat Subscription Manager (RHSM).

Você pode fazer alterações em um segredo existente por meio do Secrets Manager. Para atualizar tags ou outros metadados do seu segredo, consulte Modificar um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário. Para atualizar o valor secreto, consulte Atualizar o valor de um AWS Secrets Manager segredo.

Últimos dados sincronizados em

A data e hora da última atualização bem-sucedida dos dados de assinatura da conta registrada do Red Hat Subscription Manager (RHSM).

Tags

Você pode definir pares de valores-chave para tags que o License Manager atribui ao seu segredo de acesso RHSM no Secrets Manager. Para recuperar e descriptografar seu segredo de acesso ao RHSM, a política de função vinculada ao serviço do License Manager exige que o segredo, e qualquer associado AWS KMS key, tenha a seguinte tag atribuída:

```
"LicenseManagerLinuxSubscriptions": "enabled"
```

A tag é atribuída automaticamente se o License Manager criou seu segredo durante o processo de registro. Se você criar seu próprio segredo para o token offline, certifique-se de atribuir essa tag ao segredo e à chave KMS associada, se ela estiver criptografada. Para adicionar a tag, consulte Modificar um AWS Secrets Manager segredo no Guia AWS Secrets Manager do usuário.

Configurações de assinatura baseadas no usuário no License Manager

As configurações a seguir estão disponíveis dependendo de quais produtos você precisa para Conversão de tipo de licença.

AWS Managed Microsoft AD

O License Manager AWS Managed Microsoft AD precisa ser configurado para que você possa trabalhar com assinaturas baseadas no usuário. Para obter mais informações, consulte Use assinaturas baseadas no usuário do License Manager para produtos de software compatíveis.

Virtual private cloud

O License Manager exige que sua VPC seja configurada, além da sua AWS Managed Microsoft AD, quando você usa assinaturas baseadas em usuário com o Microsoft Office. Para obter mais informações, consulte Use assinaturas baseadas no usuário do License Manager para produtos de software compatíveis.

Configurações de administrador delegado no License Manager

É possível registrar um administrador delegado para executar tarefas administrativas para licenças gerenciadas e assinaturas do Linux no License Manager. Para simplificar a administração, recomendamos usar o console do License Manager para registrar um único administrador delegado para cada atributo do License Manager. Ao usar essa abordagem, você terá um único administrador delegado em sua organização para o License Manager.

Usando o AWS CLI ou SDKs, você pode registrar diferentes contas de membros em sua organização como administrador delegado para cada recurso suportado do License Manager. Isso faz com que diferentes contas de membros em sua organização possam realizar tarefas administrativas para licenças gerenciadas e assinaturas Linux.

> **Important**
>
> Para usar os atributos de administração delegada no console do License Manager, você deve ter a mesma conta de membro registrada como administrador delegado para cada atributo do License Manager. Se você registrou mais de uma conta de membro como administrador delegado, primeiro você precisa cancelar o registro das contas de membros existentes e, em seguida, registrar a mesma conta para cada atributo do License Manager.

Antes de registrar um administrador delegado, você deve habilitar o acesso confiança com as organizações. Para obter mais informações, consulte Convidar uma AWS conta para se juntar à sua organização e Habilitar acesso confiável com AWS Organizations.

A seguir estão os atributos para os quais você pode registrar um administrador delegado:

Licenças gerenciadas

É possível realizar tarefas administrativas, como compartilhar licenças autogerenciadas com outras contas-membro, realizar a descoberta de atributos entre contas e distribuir direitos gerenciados para outras contas-membro.

Assinaturas Linux

Você pode realizar tarefas administrativas, como visualizar e gerenciar assinaturas comerciais do Linux que você possui e administra Regiões da AWS e suas contas em. AWS Organizations Você também pode criar e gerenciar CloudWatch alarmes da Amazon para suas assinaturas Linux. Primeiro os dados devem ser descobertos e agregados antes de ficarem visíveis no console do License Manager e todos os alarmes poderem funcionar, caso estejam configurados.

> **Important**
>
> Depois de registrado, o administrador delegado tem visibilidade das instâncias do EC2 pertencentes às contas da organização.

Você pode registrar e cancelar o registro de administradores delegados usando o AWS License Manager console,, ou. AWS CLIAWS SDKs

Regiões suportadas por administradores delegados do License Manager

As seguintes regiões oferecem suporte aos administradores delegados do License Manager:

- Leste dos EUA (Ohio)
- Leste dos EUA (Norte da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Ásia-Pacífico (Hong Kong)
- Oriente Médio (Bahrein)
- Canadá (Central)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)

- Europa (Paris)
- Europa (Estocolmo)
- Europa (Milão)
- África (Cidade do Cabo)
- América do Sul (São Paulo)

Registre um administrador delegado do License Manager

Você pode registrar um administrador delegado usando o AWS CLI ou Console de gerenciamento da AWS.

Console

Para registrar um administrador delegado usando o AWS License Manager console, execute as seguintes etapas:

1. Faça login AWS como administrador da conta de gerenciamento.
2. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
3. Selecione Configurações no painel de navegação à esquerda.
4. Escolha a guia Administração delegada.
5. Selecione Registrar administrador delegado.
6. Insira a ID da conta-membro para se registrar como administrador delegado, confirme que deseja conceder ao License Manager as permissões necessárias e escolha Registrar.
7. Uma mensagem indica se a conta especificada foi registrada com sucesso como administrador delegado do License Manager.

AWS CLI

Para registrar um administrador delegado para licenças gerenciadas usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

```
aws organizations register-delegated-administrator --service-principal=license-manager.amazonaws.com --account-id=<account-id>
```

2. Execute o comando a seguir para verificar se a conta-membro especificada foi registrada com êxito como o administrador delegado.

```
aws organizations list-delegated-administrators --service-principal=license-
manager.amazonaws.com
```

Para registrar um administrador delegado para assinaturas Linux usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

```
aws organizations register-delegated-administrator --service-principal=license-
manager-linux-subscriptions.amazonaws.com --account-id=<account-id>
```

2. Execute o comando a seguir para verificar se a conta-membro especificada foi registrada com êxito como o administrador delegado.

```
aws organizations list-delegated-administrators --service-principal=license-
manager-linux-subscriptions.amazonaws.com
```

Cancele o registro de um administrador delegado do License Manager

Você pode cancelar o registro de um administrador delegado usando o ou. AWS CLI Console de gerenciamento da AWS

Console

Para cancelar o registro de um administrador delegado usando o AWS License Manager console, execute as seguintes etapas:

1. Faça login AWS como administrador da conta de gerenciamento.
2. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
3. Selecione Configurações no painel de navegação à esquerda.
4. Escolha a guia Administração delegada.
5. Escolha Remover.
6. Digite o texto **`remove`** para confirmar que quer remover o administrador delegado do License Manager e escolha Remover.

7. Uma mensagem indica se a conta especificada foi removida com sucesso como administrador delegado do License Manager.

AWS CLI

Para cancelar o registro de um administrador delegado para licenças gerenciadas usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

```
aws organizations deregister-delegated-administrator --service-
principal=license-manager.amazonaws.com --account-id=<account-id>
```

2. Execute o comando a seguir para verificar se a conta-membro especificada teve o registro cancelado com êxito como administrador delegado:

```
aws organizations list-delegated-administrators --service-principal=license-
manager.amazonaws.com
```

Para cancelar o registro de um administrador delegado para assinaturas Linux usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

```
aws organizations deregister-delegated-administrator --service-
principal=license-manager-linux-subscriptions.amazonaws.com --account-
id=<account-id>
```

2. Execute o comando a seguir para verificar se a conta-membro especificada teve o registro cancelado com êxito como administrador delegado:

```
aws organizations list-delegated-administrators --service-principal=license-
manager-linux-subscriptions.amazonaws.com
```

É possível registrar novamente uma conta cujo registro foi cancelado a qualquer momento.

Monitorar o License Manager

Você pode monitorar o uso de licenças e assinaturas rastreadas usando a Amazon. AWS License Manager CloudWatch CloudWatch coleta dados brutos e os processa em métricas legíveis, quase em tempo real. É possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte Monitorando o License Manager com a Amazon CloudWatch.

Você pode capturar chamadas de API e eventos relacionados feitos por ou em nome do seu Conta da AWS usuário AWS CloudTrail. Eventos são capturados como arquivos de log e entregues a um bucket do Amazon S3 especificado. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte Registrando chamadas de AWS License Manager API usando AWS CloudTrail.

Sumário

Monitorando o License Manager com a Amazon CloudWatch

Você pode monitorar as estatísticas métricas do License Manager usando a Amazon CloudWatch. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como a aplicação web ou o serviço está se saindo. É possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Por exemplo, é possível observar a porcentagem de licenças usando a métrica `LicenseConfigurationUsagePercentage` e agir antes que os limites sejam excedidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

O License Manager emite as seguintes métricas de hora em hora no namespace `AWSLicenseManager/licenseUsage`:

Métrica	Description
RunningInstancesCount	O número total de instâncias em execução na conta atual agrupadas pelo nome da assinatura. Unidades: contagem Dimensões: `SubscriptionName` : o nome da assinatura.
AggregateRunningInstancesCount	O número total agregado de instâncias em execução de todas as suas contas do AWS Organizations na Região da AWS atual. Unidades: contagem Dimensões: `SubscriptionName` : o nome da assinatura.
TotalLicenseConfigurationUsageCount	O número total de uma configuração de licença que pode estar disponível. Unidades: contagem Dimensões: • `LicenseConfigurationArn` : a configuração da licença do nome do recurso da Amazon (ARN). • `LicenseConfigurationType` : o tipo de configuração da licença.
LicenseConfigurationUsageCount	O número total de licenças usadas dessa configuração. Unidades: contagem Dimensões: • `LicenseConfigurationArn` : a configuração da licença do ARN. • `LicenseConfigurationType` : o tipo de configuração da licença.

Métrica	Description
LicenseConfigurationUsagePercentage	As licenças usadas dessa configuração de licença expressas em porcentagem. Unidades: percentual Dimensões: • `LicenseConfigurationArn` : a configuração da licença do ARN. • `LicenseConfigurationType` : o tipo de configuração da licença.
InstanceCount	Número de instâncias em um grupo de ativos de licença. Unidades: contagem Dimensões: • `LicenseAssetGroupArn` : O grupo de ativos de licença ARN. • `LicensingModel` : O modelo de licenciamento (LicenseIncluded ou AWSMarketplace). Disponível somente para grupos de ativos de licença com conjuntos AWS de regras gerenciados.
InstanceConsumedLicenseCount	Número de licenças consumidas para instâncias dentro de um grupo de ativos de licença. Unidades: contagem Dimensões: • `LicenseAssetGroupArn` : O grupo de ativos de licença ARN. • `LicenseCountingType` : o tipo de contagem de licenças (instância, vCPU, soquete ou núcleo). • `LicensingModel` : O modelo de licenciamento (LicenseIncluded ou AWSMarketplace). Disponível somente para grupos de ativos de licença com conjuntos AWS de regras gerenciados.

Criação de alarmes para monitorar as métricas do License Manager

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon Simple Notification Service (Amazon SNS) quando o valor da métrica muda e faz com que o alarme mude de estado. Um alarme observa uma métrica ao longo de um período especificado por você e realiza ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. Os alarmes invocam ações apenas para alterações de estado sustentado. Os alarmes do CloudWatch não invocam ações simplesmente porque estão em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte Usando CloudWatch alarmes.

Registrando chamadas de AWS License Manager API usando AWS CloudTrail

AWS License Manager é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no License Manager. CloudTrail captura todas as chamadas de API para o License Manager como eventos. Isso inclui as chamadas do console do License Manager e as chamadas de código para as operações de API do License Manager. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o License Manager. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao License Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Tópicos

- Informações do License Manager em CloudTrail
- Noções básicas sobre as entradas do arquivo de log do License Manager

Informações do License Manager em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no License Manager, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes

no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do License Manager, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do License Manager são registradas CloudTrail e documentadas na Referência da AWS License Manager API. Por exemplo, chamadas para as chamadas para o `ListResourceInventory` e `CreateLicenseConfiguration` as `DeleteLicenseConfiguration` ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre as entradas do arquivo de log do License Manager

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais

entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `DeleteLicenseConfiguration` ação.


```
{
   "eventVersion":"1.05",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDAIF2U5EXAMPLEH5AP6",
      "arn":"arn:aws:iam::123456789012:user/Administrator",
      "accountId":"012345678901",
      "accessKeyId":"AKIDEXAMPLE",
      "userName":"Administrator"
   },
   "eventTime":"2019-02-15T06:48:37Z",
   "eventSource":"license-manager.amazonaws.com",
   "eventName":"DeleteLicenseConfiguration",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.83",
   "userAgent":"aws-cli/2.4.6 Python/3.8.8 Linux",
   "requestParameters":{
      "licenseConfigurationArn":"arn:aws:license-manager:us-
east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
   },
   "responseElements":null,
   "requestID":"3366df5f-4166-415f-9437-c38EXAMPLE48",
   "eventID":"6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
   "eventType":"AwsApiCall",
   "recipientAccountId":"012345678901"
}
```

Segurança no License Manager

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O Modelo de Responsabilidade Compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao License Manager, consulte AWS Services in Scope by Compliance Program AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o License Manager. Os tópicos a seguir mostram como configurar o License Manager para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do License Manager.

Tópicos

Proteção de dados no License Manager

O AWS modelo de responsabilidade compartilhada se aplica à proteção de dados no AWS License Manager. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Perguntas frequentes sobre privacidade de dados . Para obter informações sobre proteção de dados na Europa, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (RGPD).

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o License Manager ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos

de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso

O License Manager armazena dados em um bucket do Amazon S3 na conta de gerenciamento. O bucket é configurado usando chaves de criptografia gerenciadas pelo Amazon S3 ()SSE-S3.

Gerenciamento de identidade e acesso para License Manager

AWS Identity and Access Management (IAM) é um AWS serviço que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS os recursos. Com o IAM, você pode criar usuários e grupos em sua AWS conta. Você controla as permissões que os usuários têm para realizar tarefas usando AWS recursos. Você pode usar o IAM sem custo adicional.

Por padrão, os usuários não têm permissões para usar os atributos e operações do License Manager. Para permitir que os usuários gerenciem atributos do License Manager, crie uma política do IAM que conceda permissões a eles de forma explícita.

Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos atributos especificados. Para obter mais informações, consulte Políticas e permissões no Guia do usuário do IAM.

Criar usuários, grupos e perfis

Você pode criar usuários e grupos para você Conta da AWS e, em seguida, atribuir a eles as permissões necessárias. Como prática recomendada, os usuários devem adquirir as permissões assumindo perfis do IAM. Para obter mais informações sobre como configurar usuários e grupos para a sua Conta da AWS, consulte Comece a usar o License Manager.

Um perfil do IAM é uma identidade do IAM que você pode criar em sua conta que tem permissões específicas. Uma função do IAM é semelhante à de um usuário do IAM, pois é uma AWS identidade com políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Além disso, um perfil não tem credenciais de longo prazo padrão associadas a ele, como senha ou chaves de acesso. Em vez disso, quando você assumir um perfil, ele fornecerá credenciais de segurança temporárias para sua sessão de perfil.

Estrutura da política do IAM

A política do IAM é um documento JSON que consiste em uma ou mais instruções. Cada instrução é estruturada da maneira a seguir.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Existem vários elementos que compõem uma instrução:

- Effect: o efeito pode ser `Allow` ou `Deny`. Por padrão, os usuários não têm permissão para usar atributos e operações de API. Portanto, todas as solicitações são negadas. Um permitir explícito substitui o padrão. Uma negar explícito substitui todas as permissões.
- Action: a ação é a operação de API específica para a qual você está concedendo ou negando permissão.
- Resource: o atributo afetado pela ação. Algumas operações de API do License Manager permitem que você inclua atributos específicos em sua política que podem ser criados ou modificados pela operação. Para especificar um atributo na instrução, você precisa usar o Nome do recurso da Amazon (ARN). Para obter mais informações, consulte Ações definidas por AWS License Manager.
- Condição: condições são opcionais. Elas podem ser usadas para controlar quando a política está em vigor. Para obter mais informações, consulte Uso de chaves de condição do AWS License Manager.

Criar políticas do IAM para o License Manager

Em uma instrução de política do IAM, você pode especificar qualquer operação de API de qualquer serviço que ofereça suporte ao IAM. O License Manager usa os seguintes prefixos com o nome da operação de API:

- `license-manager:`
- `license-manager-user-subscriptions:`
- `license-manager-linux-subscriptions:`

Por exemplo:

- `license-manager:CreateLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`
- `license-manager-user-subscriptions:ListIdentityProviders`
- `license-manager-linux-subscriptions:ListLinuxSubscriptionInstances`

Para obter mais informações sobre o License Manager disponível APIs, consulte as seguintes referências de API:

- AWS License Manager API Reference
- AWS License Manager Referência da API de assinaturas de usuários
- AWS License Manager Referência da API de assinaturas Linux

Para especificar várias operações em uma única instrução, separe-as com vírgulas da seguinte maneira:

```
"Action": ["license-manager:action1", "license-manager:action2"]
```

Você também pode especificar várias operações usando caracteres curinga. Por exemplo, você pode especificar todas as operações da API do License Manager cujo nome começa com a palavra List da seguinte maneira:

```
"Action": "license-manager:List*"
```

Para especificar todas as operações da API do License Manager, use o asterisco (*) conforme o seguinte:

```
"Action": "license-manager:*"
```

Exemplo de política para um ISV que usa o License Manager

ISVs que distribuem licenças por meio do License Manager exigem as seguintes permissões:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:ListLicenses",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
            "license-manager:CheckInLicense",
            "kms:GetPublicKey"
        ],
        "Resource": "*"
        }
    ]
}
```

Conceder permissões a usuários, grupos e perfis

Depois de criar as políticas do IAM necessárias, você precisa conceder essas permissões aos seus usuários, grupos e perfis.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Usando funções vinculadas a serviços para o License Manager

AWS License Manager usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao License Manager. As funções vinculadas ao serviço são predefinidas pelo License Manager e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração do License Manager porque você não precisa adicionar as permissões necessárias manualmente. O License Manager define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o License Manager pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir um perfil vinculado ao serviço somente depois de excluir os atributos relacionados. Isso protege os atributos do License Manager, pois você não pode remover por engano as permissões para acessar os atributos.

As ações do License Manager dependem de três perfis vinculados ao serviço, conforme descritos nas seções a seguir.

Perfis vinculados ao serviço

- License Manager: perfil principal

- License Manager: perfil da conta de gerenciamento
- License Manager: perfil da conta-membro
- License Manager: perfil de assinatura baseado no usuário
- License Manager: perfil de assinaturas Linux

License Manager: perfil principal

O License Manager requer um perfil vinculado ao serviço para gerenciar licenças em seu nome.

Permissões do principal perfil

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerRole` permite que o License Manager acesse AWS recursos para gerenciar licenças em seu nome.

O perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerRole` confia no serviço `license-manager.amazonaws.com` para presumir o perfil.

Para revisar as permissões do AWSLicenseManagerServiceRolePolicy, consulteAWS política gerenciada: AWSLicenseManagerServiceRolePolicy. Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte Permissões do perfil vinculado ao serviço no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço para o License Manager

Não é necessário criar manualmente um perfil vinculado ao serviço. Ao concluir o formulário de experiência de primeira execução do License Manager na primeira vez que acessar o console do License Manager, o perfil vinculado ao serviço será criada automaticamente.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você usava o License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o

perfil`AWSServiceRoleForAWSLicenseManagerRole` em sua conta. Para obter mais informações, consulte Uma novo perfil apareceu na minha conta do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Começar a usar o License Manager.
3. No formulário Permissões do IAM (one-time-setup), selecione Eu AWS License Manager concedo as permissões necessárias e escolha Continuar.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso do License Manager. Como alternativa, na AWS CLI ou na AWS API, use o IAM para criar uma função vinculada ao serviço com o nome do `license-manager.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite que você edite o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir todos os atributos usados pelo perfil. Isso significa desassociar todas as licenças autogerenciadas das instâncias associadas e AMIs, em seguida, excluir as licenças autogerenciadas.

> **Note**
>
> Se o License Manager estiver usando o perfil quando você tentar excluir os atributos, a exclusão poderá falhar. Se isso acontecer, aguarde alguns minutos e tente a ação novamente.

Para excluir atributos do License Manager usados pelo perfil vinculado ao serviço

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação, escolha Licenças autogerenciadas.
3. Escolha uma licença autogerenciada da qual você seja o proprietário e desassocie todas as entradas nas guias Associados AMIs e Recursos. Repita este processo para cada configuração de licença.
4. Ainda na página de licenças autogerenciadas, escolha Ações e, em seguida, selecione Excluir.
5. Repita as etapas anteriores até que todas as licenças autogerenciadas tenham sido excluídas.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerRole` vinculada ao serviço. Se você também estiver usando AWSServiceRoleForAWSLicenseManagerMasterAccountRolee AWSLicenseManagerMemberAccountRole, exclua essas funções primeiro. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

License Manager: perfil da conta de gerenciamento

O License Manager requer um perfil vinculado ao serviço para realizar o gerenciamento de licenças.

Permissões para o perfil da conta de gerenciamento

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` permite que o License Manager

acesse AWS recursos para gerenciar ações de gerenciamento de licenças para uma conta de gerenciamento central em seu nome.

O perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` confia no serviço `license-manager.master-account.amazonaws.com` para presumir o perfil.

Para revisar as permissões do AWSLicenseManagerMasterAccountRolePolicy, consulteAWS política gerenciada: AWSLicenseManagerMasterAccountRolePolicy. Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte Permissões do perfil vinculado ao serviço no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço para a conta de gerenciamento

Você não precisa criar manualmente esse perfil vinculado ao serviço. Quando você configura o gerenciamento de licenças entre contas no Console de gerenciamento da AWS, o License Manager cria a função vinculada ao serviço para você.

> **Note**
>
> Para usar o suporte entre contas no License Manager, você deve estar usando AWS Organizations.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você usava o License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` em sua conta. Para obter mais informações, consulte Uma novo perfil apareceu na minha conta do IAM.

Você pode usar o console do License Manager para criar esse perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. Escolha Configurações, Editar.
3. Escolha Vincular AWS Organizations contas.
4. Escolha Aplicar.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso de conta de gerenciamento do License Manager. Como alternativa, na AWS CLI ou na AWS API, use o IAM para criar uma função vinculada ao serviço com o nome do `license-manager.master-account.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMasterAccountRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

License Manager: perfil da conta-membro

O License Manager requer um perfil vinculado ao serviço que permita o gerenciamento de contas para gerenciar licenças.

Permissões para o perfil da conta-membro

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` permite que o License Manager acesse AWS recursos para ações de gerenciamento de licenças a partir de uma conta de gerenciamento configurada em seu nome.

O perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` confia no serviço `license-manager.member-account.amazonaws.com` para presumir o perfil.

Para revisar as permissões do AWSLicenseManagerMemberAccountRolePolicy, consulteAWS política gerenciada: AWSLicenseManagerMemberAccountRolePolicy. Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte Permissões do perfil vinculado ao serviço no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço. Você pode ativar a integração com AWS Organizations a conta de gerenciamento no console do License Manager na página Configurações. Você também pode fazer isso usando a AWS CLI (executar`update-service-settings`) ou a AWS API (chamada`UpdateServiceSettings`). Ao fazer isso, o License Manager cria o perfil vinculado ao serviço para você nas contas-membro do Organizations.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou AWS CLI a AWS API para criar manualmente uma função vinculada ao serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você

usava o serviço do License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o perfil`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` em sua conta. Para obter mais informações, consulte Uma novo perfil apareceu na minha conta do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Faça login na sua conta AWS Organizations de gerenciamento.
2. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
3. Na barra de navegação à esquerda, escolha Configurações e, em seguida, escolha Básico.
4. Escolha Vincular AWS Organizations contas.
5. Escolha Aplicar. Isso cria as funções AWSServiceRoleForAWSLicenseManagerRolee AWSServiceRoleForAWSLicenseManagerMemberAccountRoleem todas as contas infantis.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso `License Manager - Member account`. Como alternativa, na AWS API AWS CLI ou, crie uma função vinculada ao serviço com o nome do `license-manager.member-account.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMemberAccountRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você ficará somente com entidades que sejam monitoradas

ou mantidas ativamente. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

License Manager: perfil de assinatura baseado no usuário

O License Manager exige uma função vinculada ao serviço para gerenciar AWS recursos que fornecerão assinaturas baseadas no usuário.

Permissões para o perfil de assinatura baseada no usuário

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` permite que o License Manager utilize AWS Systems Manager e gerencie recursos do Amazon EC2 fornecendo assinaturas baseadas no usuário, bem como descreva recursos. Directory Service

Para revisar as permissões do AWSLicenseManagerUserSubscriptionsServiceRolePolicy, consulteAWS política gerenciada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy.
Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte Permissões do perfil vinculado ao serviço no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço, pois você será solicitado nas páginas de assinaturas baseadas no usuário do console do License Manager para criar o perfil.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.
2. No painel de navegação à esquerda, escolha Associação de usuário ou Produtos.
3. Concorde com os termos do License Manager para criar o perfil de assinatura baseada no usuário.
4. Escolha Criar. Isso cria o perfil.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso `License Manager - User-based subscriptions`. Como alternativa, na AWS API AWS CLI ou, crie uma função vinculada ao serviço com o nome do `license-manager-user-subscriptions.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

License Manager: perfil de assinaturas Linux

O License Manager exige uma função vinculada ao serviço para gerenciar AWS recursos que fornecem assinaturas Linux.

Permissões para o perfil de assinaturas Linux

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` permite que o License Manager execute as seguintes ações para assinaturas Linux.

- Conheça a Amazon Elastic Compute Cloud e AWS Organizations os recursos.
- Recupere segredos marcados com `"LicenseManagerLinuxSubscriptions": "enabled"` de AWS Secrets Manager para acessar provedores de assinatura Linux terceirizados para obter informações de assinatura.
- Use as chaves KMS marcadas com `"LicenseManagerLinuxSubscriptions": "enabled"` para descriptografar segredos.

Para revisar as permissões do AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy, consulteAWS política gerenciada: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy. Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte Permissões do perfil vinculado ao serviço no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço, pois você será solicitado nas páginas de assinaturas Linux do console do License Manager para criar o perfil.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em https://console.aws.amazon.com/license-manager/.

2. No painel de navegação à esquerda, escolha Assinaturas ou Instâncias.
3. Concorde com os termos do License Manager para criar o perfil de assinaturas Linux.
4. Escolha Criar. Isso cria o perfil.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso `License Manager - Linux subscriptions`. Como alternativa, na AWS API AWS CLI ou, crie uma função vinculada ao serviço com o nome do `license-manager-linux-subscriptions.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

AWS políticas gerenciadas para License Manager

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam.

Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AWSLicenseManagerServiceRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de `AWSServiceRoleForAWSLicenseManagerRole` para permitir que o License Manager chame ações da API para gerenciar licenças para você. Para saber mais sobre a função vinculada ao serviço do , consulte Permissões do principal perfil.

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
`iam:CreateServiceLinkedRole`	`arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleFor`

Ação	Atributo ARN
	MarketplaceLicense Management
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*

Ação	Atributo ARN
ssm:CreateAssociation	*
ssm:GetCommandInvocation	*
ssm:SendCommand	arn:aws:ec2:*:*:instance/*
ssm:SendCommand	arn:aws:ssm:*:*:managed-instance/*
ssm:SendCommand	arn:aws:ssm:*::document/AWSLicenseManager-*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

Para ver as permissões dessa política no Console de gerenciamento da AWS, consulte AWSLicenseManagerServiceRolePolicy.

AWS política gerenciada: AWSLicenseManagerMasterAccountRolePolicy

Essa política é anexada à função vinculada ao serviço nomeada `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` para permitir que o License Manager chame ações de API que realizam o gerenciamento de licenças para uma conta de

gerenciamento central em seu nome. Para saber mais sobre a função vinculada ao serviço do , consulte License Manager: perfil da conta de gerenciamento.

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:GetBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*

Ação	Atributo ARN
s3:DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	Consulte a nota de rodapé [1]
glue:UpdateTable	Consulte a nota de rodapé [1]
glue:DeleteTable	Consulte a nota de rodapé [1]
glue:UpdateJob	Consulte a nota de rodapé [1]
glue:UpdateCrawler	Consulte a nota de rodapé [1]
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*

Ação	Atributo ARN
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram:DeleteResourceShare	*
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

Ação	Atributo ARN
`cloudformation:DeleteStack`	`arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*`
`cloudformation:DescribeStacks`	`arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*`

[1] A seguir estão os recursos definidos para as AWS Glue ações:

- `arn:aws:glue:*:*:catalog`
- `arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler`
- `arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob`
- `arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*`
- `arn:aws:glue:*:*:table/license_manager_resource_sync/*`
- `arn:aws:glue:*:*:database/license_manager_resource_inventory_db`
- `arn:aws:glue:*:*:database/license_manager_resource_sync`

Para ver as permissões dessa política no Console de gerenciamento da AWS, consulte AWSLicenseManagerMasterAccountRolePolicy.

AWS política gerenciada: AWSLicenseManagerMemberAccountRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` para permitir que o License Manager chame ações de API para gerenciar licenças de uma conta de gerenciamento para você. Para obter mais informações, consulte License Manager: perfil da conta-membro.

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
`license-manager:UpdateLicenseSpecificationsForResource`	*
`license-manager:GetLicenseConfiguration`	*
`ssm:ListInventoryEntries`	*
`ssm:GetInventory`	*
`ssm:CreateAssociation`	*
`ssm:CreateResourceDataSync`	*
`ssm:DeleteResourceDataSync`	*
`ssm:ListResourceDataSync`	*
`ssm:ListAssociations`	*
`ram:AcceptResourceShareInvitation`	*
`ram:GetResourceShareInvitations`	*

Para ver as permissões dessa política no Console de gerenciamento da AWS, consulte AWSLicenseManagerMemberAccountRolePolicy.

AWS política gerenciada: AWSLicenseManagerConsumptionPolicy

É possível anexar a política `AWSLicenseManagerConsumptionPolicy` às suas identidades do IAM. Essa política concede permissões que permitem acesso às ações da API do License Manager necessárias para consumir licenças. Para obter mais informações, consulte Uso da licença emitida pelo vendedor no License Manager.

Para visualizar as permissões para esta política, consulte AWSLicenseManagerConsumptionPolicy no Console de gerenciamento da AWS.

AWS política gerenciada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de política da `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` para permitir que o License Manager chame ações de API para gerenciar atributos de licenças baseadas no usuário. Para obter mais informações, consulte License Manager: perfil de assinatura baseado no usuário.

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
anúncios: DescribeDirectories	*
anúncios: GetAuthorizedApplicationDetails	*
ec2: CreateTags	arn:aws:ec2:*:*:instance/* [1]
ec2: DescribeInstances	*
ec2: DescribeNetworkInterfaces	*
ec2: DescribeSecurityGroupRules	*
ec2: DescribeSubnets	*
ec2: DescribeVpcPeeringConnections	*
ec2: TerminateInstances	arn:aws:ec2:*:*:instance/* [1]
rota 53: GetHostedZone	*
rota 53: ListResourceRecordSets	*
gerente de segredos: GetSecretValue	arn:aws:secretsmanager: *:*:secret: -* license-manager-user
sms: DescribeInstanceInformation	*
sms: GetCommandInvocation	*

Ação	Atributo ARN
sms: GetInventory	*
sms: ListCommandInvocations	*
sms: SendCommand	arn:aws:ssm: *:document/aws-[2] RunPowerShellScript arn:aws:ec2:*:*:instance/* [2]

[1] O License Manager só pode criar tags e encerrar instâncias que tenham os códigos de produto bz0vcy31ooqlzk5tsash4r1ik, 77yzkpa7kvee1y1tt7wnsdwoc, d44g89hc0gp9jdzm99rznthpw ou 5uypd9kpy863kwykrwn4bcolv.

[2] O License Manager só pode executar um comando SSM Run com o documento do `AWS-RunPowerShellScript` em instâncias com o nome da tag `AWSLicenseManager` e um valor de `UserSubscriptions`.

Para ver as permissões dessa política no Console de gerenciamento da AWS, consulte AWSLicenseManagerUserSubscriptionsServiceRolePolicy.

AWS política gerenciada: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de política da `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` para permitir que o License Manager chame ações da API para gerenciar atributos de licenças Linux. Para obter mais informações, consulte License Manager: perfil de assinaturas Linux.

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Condições	Recurso
`ec2:DescribeInstances`	N/D	*
`ec2:DescribeRegions`	N/D	*

Ação	Condições	Recurso
`organizations:DescribeOrganization`	N/D	*
`organizations:ListAccounts`	N/D	*
`organizations:DescribeAccount`	N/D	*
`organizations:ListChildren`	N/D	*
`organizations:ListParents`	N/D	*
`organizations:ListAccountsForParent`	N/D	*
`organizations:ListRoots`	N/D	*
`organizations:ListAWSServiceAccessForOrganization`	N/D	*
`organizations:ListDelegatedAdministrators`	N/D	*
gerente de segredos: GetSecretValue	StringEquals: “aws:ResourceTag/LicenseManagerLinuxSubscriptions“: “ativado” “aws: ResourceAccount “: “${aws:PrincipalAccount}”	`arn:aws:secretsmanager:*:*:secret:*`

Ação	Condições	Recurso
kms:Decrypt	StringEquals: “aws:ResourceTag/LicenseManagerLinuxSubscriptions“: “ativado”, “aws: ResourceAccount “: “${aws:PrincipalAccount}” StringLike: “kms: “: [ViaService“secretsmanager.*.amazonaws.com”]	`arn:aws:kms:*:*:key/*`

Para ver as permissões dessa política no Console de gerenciamento da AWS, consulte AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy.

Atualizações do License Manager para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do License Manager desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – atualização para uma política existente	O License Manager adicionou os seguintes códigos de produto à lista de códigos de produto em instâncias para as quais o License Manager pode criar tags e encerrar instâncias: 5uypd9kpy863kwykrwn4bcolv.	13 de abril de 2026
AWSLicenseManagerServiceRolePolicy – atualização para uma política existente	O License Manager adicionou permissões para descobrir ativos de licença em instância	19 de novembro de 2025

Alteração	Descrição	Data
	s executando documentos SSM gerenciados pela AWS.	
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – atualização para uma política existente	O License Manager adicionou as seguintes permissões para gerenciar o licenciamento e os dados do Active Directory: obter informações de rota do Route 53, obter informações de rede e regras de grupos de segurança do Amazon EC2 e obter segredos do Secrets Manager.	7 de novembro de 2024
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – atualização para uma política existente	O License Manager adicionou permissões para armazenar e recuperar segredos e usar AWS KMS chaves para descriptografar segredos de AWS Secrets Manager token de acesso para assinatur as Bring Your Own License (BYOL).	22 de maio de 2024
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – Nova política	O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` . Essa função fornece ao License Manager permissão para listar recursos AWS Organizations e recursos do Amazon EC2.	21 de dezembro de 2022

Alteração	Descrição	Data
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – atualização para uma política existente	O License Manager adicionou a permissão do `ec2:DescribeVpcPeeringConnections` .	28 de novembro de 2022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – Nova política	O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de `AWSLicenseManagerUserSubscriptionsServiceRolePolicy` . Essa função fornece ao License Manager permissão para listar AWS Directory Service recursos, utilizar recursos do Systems Manager e gerenciar recursos do Amazon EC2 criados para assinaturas baseadas em usuários.	18 de julho de 2022
AWSLicenseManagerMasterAccountRolePolicy – atualização para uma política existente	O License Manager adicionou a `resource-groups:PutGroupPolicy` permissão para grupos de recursos gerenciados por AWS Resource Access Manager.	27 de junho de 2022

Alteração	Descrição	Data
AWSLicenseManagerMasterAccountRolePolicy – atualização para uma política existente	O License Manager alterou a chave de `AWSLicenseManagerMasterAccountRolePolicy` condição da política AWS AWS Resource Access Manager gerenciada de usar `ram:ResourceTag` para `aws:ResourceTag` .	16 de novembro de 2021
AWSLicenseManagerConsumptionPolicy – Nova política	O License Manager adicionou uma nova política que concede permissões para consumir licenças.	11 de agosto de 2021
AWSLicenseManagerServiceRolePolicy – atualização para uma política existente	O License Manager adicionou uma permissão para listar administradores delegados e uma permissão para criar o perfil vinculado ao serviço chamado `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` .	16 de junho de 2021
AWSLicenseManagerServiceRolePolicy – atualização para uma política existente	O License Manager adicionou uma permissão para listar todos os atributos do License Manager, como configurações de licenças, licenças e concessões.	15 de junho de 2021

Alteração	Descrição	Data
AWSLicenseManagerServiceRolePolicy – atualização para uma política existente	O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de `AWSServiceRoleForMarketplaceLicenseManagement` . Essa função AWS Marketplace fornece permissões para criar e gerenciar licenças no License Manager. Para obter mais informações, consulte perfis vinculados ao serviço para o AWS Marketplace no Guia do comprador do AWS Marketplace .	9 de março de 2021
O License Manager começou a rastrear as alterações	O License Manager começou a monitorar as alterações em suas políticas AWS gerenciadas.	9 de março de 2021

Assinatura criptográfica de licenças no License Manager

O License Manager pode assinar criptograficamente licenças emitidas por um ISV ou AWS Marketplace em nome de um ISV. A assinatura permite que os fornecedores validem a integridade e a origem de uma licença dentro do próprio aplicativo, mesmo em um ambiente offline.

Para assinar licenças, o License Manager usa uma assimétrica AWS KMS key pertencente a um ISV e protegida em (). AWS Key Management Service AWS KMS Essa CMK gerenciada pelo cliente consiste em um par de chave pública e chave privada relacionadas matematicamente. Quando um usuário solicita uma licença, o License Manager gera um objeto JSON listando os direitos da licença e assina o objeto com a chave privada. A assinatura e o objeto JSON de texto simples são retornados ao usuário. Qualquer pessoa apresentada com esses objetos pode usar a chave pública para validar se o texto da licença não foi alterado e se a licença foi assinada pelo proprietário da

chave privada. A parte privada do par de chaves nunca sai AWS KMS. Para obter mais informações sobre criptografia assimétrica em AWS KMS, consulte Usando chaves simétricas e assimétricas.

> **Note**
>
> O License Manager chama as operações AWS KMS `Sign`e a `Verify`API ao assinar e verificar licenças. A CMK deve ter um valor de uso de chave de SIGN_VERIFY para ser usada por essas operações. Essa variedade de CMK não pode ser usada para criptografia e descriptografia.

O fluxo de trabalho a seguir descreve a emissão de licenças assinadas criptograficamente:

1. No AWS KMS console, na API ou no SDK, o administrador da licença cria uma CMK assimétrica gerenciada pelo cliente. A CMK deve usar um sinal para a chave, verificar e dar suporte ao algoritmo de assinatura RSASSA-PSS SHA-256. Para obter mais informações, consulte Criação assimétrica CMKs e Como escolher sua configuração de CMK.
2. No License Manager, o administrador da licença cria uma configuração de consumo que inclui um AWS KMS ARN ou ID. A configuração pode especificar uma ou ambas as opções de Empréstimo e provisória. Para obter mais informações, consulte Criar um bloco de licenças emitidas pelo vendedor.
3. Um usuário final obtém a licença usando a operação de API `CheckoutLicense` ou `CheckoutBorrowLicense`. A operação `CheckoutBorrowLicense` é permitida somente em licenças com o Borrow configurado. Ela retorna uma assinatura digital como parte de sua resposta junto com o objeto JSON listando os direitos. O texto simples do JSON é semelhante ao seguinte:

```
{
   "entitlementsAllowed":[
      {
         "name":"EntitlementCount",
         "unit":"Count",
         "value":"1"
      }
   ],
   "expiration":"2020-12-01T00:47:35",
   "issuedAt":"2020-11-30T23:47:35",
   "licenseArn":"arn:aws:license-
manager::123456789012:license:l-6585590917ad46858328ff02dEXAMPLE",
   "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
```

```
   "nodeId":"100.20.15.10",
   "checkoutMetadata":{
      "Mac":"ABCDEFGHI"
   }
}
```

Validação de conformidade para License Manager

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a Documentação AWS de segurança.

Resiliência no License Manager

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura no License Manager

Como serviço gerenciado, AWS License Manager é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura,

consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o License Manager pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

License Manager e interface de VPC endpoints com AWS PrivateLink

Você pode estabelecer uma conexão privada entre a nuvem privada virtual (VPC) e o AWS License Manager criando um endpoint da VPC de interface. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que você pode usar para acessar de forma privada a API do License Manager sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. Direct Connect As instâncias na VPC não precisam de endereços IP públicos para a comunicação com o License Manager. O tráfego entre sua VPC e o License Manager não deixa a rede da Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para obter mais informações, consulte Endpoints da VPC da interface (AWS PrivateLink) no Manual do Usuário do Amazon VPC.

Criar um endpoint da VPC de interface para o License Manager

Crie um endpoint de interface para o License Manager usando um dos seguintes nomes de serviço:

- com.amazonaws. ***region***.gerenciador de licenças
- com.amazonaws. ***region***. license-manager-fips

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o License Manager usando seu nome DNS padrão para a região. Por exemplo, `.license-manager.`*`region`*`.amazonaws.com`

Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Criar uma política de endpoint da VPC para o License Manager

É possível anexar uma política ao endpoint da VPC para controlar o acesso ao License Manager. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações
- As ações que podem ser executadas
- O atributo no qual as ações podem ser executadas

Veja a seguir um exemplo de uma política de endpoint para o License Manager. Quando anexada a um endpoint, essa política concede acesso às ações indicadas do License Manager para todas as entidades principais em todos os atributos.

```
{
   "Statement": [
        {
            "Principal": "*",
            "Effect": "Allow",
            "Action": [
              "license-manager:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia do usuário da Amazon VPC.

Solução de problemas do License Manager

As informações a seguir podem ajudar você a solucionar problemas ao usar o AWS License Manager. Antes de começar, confirme se a configuração do License Manager atende aos requisitos estabelecidos em the section called “Configurações”.

Erro de descoberta entre contas

Enquanto configura a descoberta entre contas, você pode encontrar a seguinte mensagem de erro na página Pesquisar inventário:

Exceção do Athena: falha na consulta do Athena devido a permissões insuficientes para executar a consulta. Migre seu catálogo para habilitar o acesso a esse banco de dados.

Isso pode ocorrer quando o serviço do Athena usa o catálogo de dados gerenciado pelo Athena, em vez do AWS Glue Data Catalog. Para obter instruções de atualização, consulte Atualização para o AWS Glue Data Catalog Step-by-Step.

A conta de gerenciamento não pode dissociar recursos de uma licença autogerenciada

Se uma conta-membro de uma organização excluir o perfil vinculado ao serviço (SLR) `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` da conta, e houver atributos pertencentes ao membro associados a uma licença autogerenciada, a gestão da conta será impedida de desassociar licenças desses atributos da conta-membro. Isso significa que os atributos da conta-membro continuarão a consumir licenças do grupo de contas de gerenciamento. Para permitir que a conta de gerenciamento desassocie atributos, restaure a SLR.

Esse comportamento é responsável por casos em que um cliente prefere não permitir que a conta de gerenciamento execute algumas ações que afetam os atributos da conta-membro.

O inventário do Systems Manager está desatualizado

O Systems Manager armazena dados nos dados de Inventário por 30 dias. Durante esse período, o License Manager conta uma instância gerenciada como ativa até mesmo se ela não for compatível

com ping. Assim que os dados de inventário forem eliminados do Systems Manager, o License Manager marcará a instância como inativa e atualizará os dados de inventário local. Para manter as contagens de instâncias gerenciadas precisas, recomendamos cancelar o registro das instâncias manualmente no Systems Manager, para que o License Manager possa executar operações de limpeza.

Persistência aparente de uma AMI de registro cancelado

O License Manager elimina associações obsoletas entre atributos e licenças autogerenciadas uma vez a cada algumas horas. Se uma AMI associada a uma licença autogerenciada tiver o registro cancelado por meio do Amazon EC2, a AMI poderá brevemente continuar a ser exibida no inventário de atributos do License Manager antes de ser removida.

Nova instância de conta filho demora a ser exibida no inventário de atributos

Quando o suporte entre contas está habilitado, o License Manager atualiza as contas do cliente às 13h diariamente por padrão. As instâncias adicionadas posteriormente no dia serão exibidas na conta de gerenciamento do inventário de atributos no dia seguinte. Você pode alterar a frequência com que o script de atualização é executado editando o `LicenseManagerResourceSynDataProcessJobTrigger` no AWS Glue console da conta de gerenciamento.

Após habilitar o modo entre contas, as instâncias de contas filho demoram a ser exibidas

Quando você habilita o modo entre contas no License Manager, as instâncias em contas filho podem levar de alguns minutos a algumas horas para serem exibidas no inventário de atributos. O tempo depende do número de contas filho e do número de instâncias em cada conta filho.

Não é possível desabilitar a descoberta entre contas

Após uma conta ser configurada para a descoberta entre contas, será impossível reverter para a descoberta em uma única conta.

O usuário de uma conta filho não consegue associar a licença autogerenciada compartilhada com uma instância

Quando isso ocorrer e a descoberta entre contas estiver habilitada, verifique o seguinte:

- Se a conta filho foi removida da organização.
- A conta filho foi removida do compartilhamento de atributos criado na conta de gerenciamento.
- A licença autogerenciada foi removida do compartilhamento de atributos.

Falha na vinculação de AWS Organizations contas

Se a página Settings (Configurações) relatar esse erro, isso indicará que uma conta não é membro de uma organização pelos seguintes motivos:

- Uma conta filho foi removida da organização.
- Um cliente desativou o acesso ao License Manager do console da organização da conta de gerenciamento.

Histórico de documentos para License Manager

A tabela a seguir descreve as versões do AWS License Manager.

Alteração	Descrição	Data
Foi adicionado suporte para assinaturas baseadas no usuário do Microsoft Office LTSC Standard	O License Manager adicionou suporte para gerenciamento e configuração de licenças fornecidas pela Amazon para o Microsoft Office LTSC Standard no Amazon EC2.	14 de abril de 2026
Suporte adicionado para o License Asset Group	O License Manager adicionou suporte para descobrir ativos de licenças e uso de software por meio de grupos de ativos de licenças. Isso inclui uma atualização para AWS política gerenciada: AWSLicens eManagerServiceRolePolicy o.	19 de novembro de 2025
Foi adicionado suporte para assinaturas baseadas no usuário do Microsoft Remote Desktop Services Subscriber Access Licenses (RDS SAL)	O License Manager adicionou suporte para gerenciamento e configuração de assinaturas baseadas no usuário do RDS SAL, incluindo a capacidad e de configurar mais de duas conexões de desktop remoto ao mesmo tempo.	14 de novembro de 2024
Política gerenciada por SLR de assinaturas com base no usuário atualizada para obter informações de rota e rede	O License Manager adicionou as seguintes permissões para gerenciar o licenciam ento e os dados do Active Directory: obter informações de rota do Route 53, obter	7 de novembro de 2024

Alteração	Descrição	Data
	informações de rede e regras de grupos de segurança do Amazon EC2 e obter segredos do Secrets Manager. Para obter mais informaçõ es, AWS política gerenciad a: AWSLicenseManagerU serSubscriptionsServiceRole Policy.	
Recupere informações de assinatura BYOL do Red Hat Subscription Manager (RHSM)	O License Manager adicionou suporte para recuperar informações de assinatura do RHSM para licenças BYOL em instâncias do Red Hat Enterprise Linux. Isso inclui atualizações para AWSLicens eManagerLinuxSubscriptionsS erviceRolePolicyo.	10 de julho de 2024
Suporte adicional para Amazon RDS para licenças BYOL baseadas em vCPUs do Db2	O License Manager adicionou suporte ao Amazon RDS para licenças BYOL baseadas em vCPUs do Db2.	20 de março de 2024
Adição do suporte ao Windows Server 2019 para assinaturas baseadas no usuário do Microsoft Office	AWS adicionou suporte para o Windows Server 2019 nas Amazon Machine Images (AMIs) com licenças fornecidas pela Amazon para o Microsoft Office LTSC Professional Plus no Amazon EC2.	4 de dezembro de 2023

Alteração	Descrição	Data
Usuários do domínio autogerenciado (on-premises) podem utilizar assinaturas baseadas em usuários	O License Manager adicionou suporte para usuários no domínio autogerenciado do Active Directory utilizare m assinaturas baseadas em usuários quando uma relação de confiança com seu AWS Managed Microsoft AD diretório for criada.	6 de setembro de 2023
Conversões de tipo de licença para assinaturas do Ubuntu LTS	O License Manager adicionou suporte para as instância s do Ubuntu LTS usarem a conversão de tipo de licença para adicionar uma assinatura do Ubuntu Pro.	20 de abril de 2023
Substituição de concessões ativas	O License Manager adicionou uma funcionalidade para substituir, opcionalmente, concessões ativas por uma licença concedida durante a ativação da concessão.	31 de março de 2023
Administração delegada para assinaturas Linux	O License Manager adicionou suporte a administradores delegados para assinaturas Linux.	3 de março de 2023
Assinaturas Linux	O License Manager adicionou o rastreamento para assinatur as comerciais Linux.	21 de dezembro de 2022

Alteração	Descrição	Data
CloudWatch Métricas da Amazon	O License Manager agora emite CloudWatch métricas para o uso da configuração de licenças e assinaturas.	21 de dezembro de 2022
Microsoft Office para assinaturas baseadas em usuários	O License Manager adicionou o Microsoft Office como software compatível com assinaturas baseadas em usuários.	28 de novembro de 2022
Distribuição de direitos às unidades organizacionais	Distribua direitos para uma OU específica em sua organização.	17 de novembro de 2022
Visualização organizacional (console)	Gerencie as licenças concedidas em suas contas AWS Organizations usando o console do License Manager.	11 de novembro de 2022
Conversão de tipo de licença	Utilize produtos com suporte a Conversão de tipo de licençano Amazon EC2.	2 de agosto de 2022
Registro e envio de dados de uso da licença (console)	Registre e envie dados de uso da licença usando o console do License Manager.	28 de março de 2022
Conversão de tipo de licença (console)	Altere seu tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) usando o console do License Manager sem reimplantar suas cargas de trabalho existentes.	9 de novembro de 2021

Alteração	Descrição	Data
Conversão de tipo de licença (CLI)	Altere seu tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) usando o AWS CLI sem reimplantar suas cargas de trabalho existentes.	22 de setembro de 2021
Compartilhamento de direitos	Compartilhe direitos de licença gerenciada com toda a sua organização com uma única solicitação.	16 de julho de 2021
Relatórios de uso	Acompanhe o histórico das configurações do seu tipo de licença com os relatórios de uso do License Manager. Anteriormente, os relatório s de uso eram chamados de geradores de relatórios e relatórios de licenças.	18 de maio de 2021
Regras de exclusão da descoberta automática	Exclua instâncias da descoberta automática do License Manager com base na AWS conta IDs e nas tags.	5 de março de 2021
Direitos gerenciados	Rastreie e distribua direitos de licença para produtos comprados AWS Marketpla ce e vendedores que usam o License Manager para distribui r licenças.	3 de dezembro de 2020

Alteração	Descrição	Data
Contabilidade automática para software desinstalado	Configure a descoberta automática para interromper o rastreamento de instâncias quando o software for desinstalado.	3 de dezembro de 2020
Filtragem por tags	Pesquise no seu inventário de atributos usando tags.	3 de dezembro de 2020
Escopo de associação do AMI	Associe suas licenças autogerenciadas e as AMIs compartilhadas à sua AWS conta.	23 de novembro de 2020
Afinidade de licença com o host	Imponha a atribuição de licenças a hardware dedicado por um número específico de dias.	12 de agosto de 2020
Rastreamento de implantações do Oracle no Amazon RDS	Rastreie o uso da licença para edições de mecanismos e pacotes de licença da base de dados do Oracle no Amazon RDS.	23 de março de 2020
Grupos de atributos de host	Configure um grupo de recursos de host para permitir que o License Manager gerencie seus hosts dedicados.	1.º de dezembro de 2019

Alteração	Descrição	Data
Descoberta automática de software	Configure o License Manager para pesquisar sistemas operacionais ou aplicativos recém-instalados e anexar as licenças autogerenciadas correspondentes às instância s.	1.º de dezembro de 2019
Diferença entre a licença incluída e Bring Your Own License	Filtre os resultados de pesquisa com base no fato de você estar usando licenças fornecidas pela Amazon ou suas próprias licenças.	8 de novembro de 2019
Anexar licenças a atributos on-premises	Depois de anexar licenças a uma instância on-premis es, o License Manager coleta periodicamente o inventári o de software, atualiza as informações de licenciamento e cria relatórios de uso.	8 de março de 2019
AWS License Manager lançamento inicial	Lançamento do serviço inicial	28 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.